

Critical Infrastructure & Key Resources

Using Commercialization to Develop Solutions
Efficiently and Effectively

January 2010

Editors:

Office of Infrastructure Protection
National Protection and Programs Directorate

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer



Homeland
Security

Critical Infrastructure & Key Resources

"Using Commercialization to Develop Solutions
Efficiently and Effectively"

January 2010

Editors:

Office of Infrastructure Protection
National Protections and Programs Division
U.S. Department of Homeland Security

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
U.S. Department of Homeland Security
Science and Technology Directorate



**Homeland
Security**

December 2009

Research and development (R&D) plays a significant role in enabling homeland security partners to develop knowledge and technologies to more effectively reduce risk to the Nation's critical infrastructure and key resources (CIKR). The Office of Infrastructure Protection in the Department of Homeland Security (DHS) is pleased to provide the CIKR Requirements book to our partners so that they may better understand the requirements process and the role of the DHS Science & Technology Directorate (S&T).

The book contains a wide range of information on how to develop detailed operational requirements, including real-world examples of the operational requirements document used by the S&T Commercialization Office. It also contains timely information on S&T's recently implemented commercialization initiative to effectively and efficiently develop products and services to help CIKR sectors meet their many challenges.

The Office of Infrastructure Protection's R&D Team will continue to work with S&T to best address the capability gaps articulated by the 18 CIKR Sectors. The S&T Commercialization Office has long been a strong partner to the R&D Team, and supports numerous initiatives (detailed throughout the book), that may enable CIKR stakeholders to quickly address key technology needs. It is our hope that CIKR stakeholders will be better equipped to capitalize on the benefits of the processes covered in this book, and continue to develop strong R&D partnerships across the Department.

Any questions regarding the information contained in this book may be directed to the IP Research and Development Team at: IPR&D@HQ.DHS.GOV

Sincerely,

A handwritten signature in blue ink that reads "Todd M. Keil". The signature is fluid and cursive, with a large initial "T" and "K".

Todd M. Keil
Assistant Secretary
Office of Infrastructure Protection
U.S. Department of Homeland Security

DHS Office of Infrastructure Protection

Protecting the nation's critical infrastructure and key resources (CIKR) is a key Department of Homeland Security mission established in 2002 by the National Strategy for Homeland Security and the Homeland Security Act.

The Department's Office of Infrastructure Protection (IP) within the National Protection and Programs Directorate (NPPD) leads the coordinated national program to reduce risks to the nation's CIKR posed by acts of terrorism and to strengthen national preparedness, timely response and rapid recovery in the event of an attack, natural disaster or other emergency.

IP addresses these needs through the National Infrastructure Protection Plan (NIPP). The NIPP establishes a partnership structure for coordination across 18 CIKR Sectors and a risk management framework to identify assets, systems, networks and functions whose loss or compromise pose the greatest risk.

Within the sector framework, IP works with public and private partners coordinating efforts to protect CIKR and provide CIKR functions to strengthen incident response. IP initiatives fall into six programmatic areas:

- Partnerships, Outreach and Training
- Contingency Planning and Incident Management
- Chemical Facility Security and Compliance
- CIKR Protective Security and Field Operations
- Infrastructure Analysis, Research and Development
- Infrastructure Information Collection and Protection

IP relies on regular interaction with CIKR owners and operators to ensure the ability of infrastructure protection personnel to conduct their missions successfully. IP also assists in addressing the needs and concerns of those infrastructure protection communities to maintain high levels of operational readiness.

Table of Contents

DHS Office of Infrastructure Protection.....	2
Table of Contents.....	3
List of Figures.....	4
Introduction.....	5
National Protection and Programs Directorate and the Office of Infrastructure Protection	7
DHS Science and Technology Directorate.....	11
Product Realization through Requirements Articulation.....	21
Why Requirements?.....	22
The Requirements Hierarchy and Traceability	24
Characteristics of Good Requirements	27
Developing Operational Requirements (ORDs): Customer Input	27
Addressing Requirements versus Proposing Solutions	33
Operational Requirements Document Template	35
DHS Markets Create Opportunities for the Private Sector	39
Summary.....	46
Additional Requirements Development Readings.....	46
Appendix A: National Infrastructure Protection Plan	49
Appendix B: ORD Examples	238
OPERATIONAL REQUIREMENTS DOCUMENT Template.....	241
Portable Stand Alone Water Purification	246
Blast Resistant Autonomous Video Equipment (BRAVE).....	254
Predictive Modeling for Counter-Improvised Explosive Devices.....	263
Appendix C: DHS S&T Infrastructure and Geophysical Division (IGD) Brief	275
Appendix D: Bridging the Communications Gap (Article)	287
Appendix E: DHS: Leading the Way to Help the Private Sector Help Itself (Article).....	296
Appendix F: SECURE™ Program (Article).....	303
Appendix G: FutureTECH™ Program (Article).....	307
Appendix H: Focus on Small Business	317
Appendix I: Commercialization Briefing to Industry	320
Appendix J: Acquisition Training Mini-Course	349
Appendix K: Creating Change to Drive Results (Brief)	373
Appendix L: Demonstrating Efficiency Brief.....	383
Appendix M: DHS S&T High Priority Technology Needs	391

Appendix N: Market Potential Templates	418
Appendix O: Product Realization Chart	422

List of Figures

Figure 1. The NIPP Partnership Model.....	8
Figure 2 The Capstone IPT model.	13
Figure 3 The thirteen Capstone IPTs.....	14
Figure 4 Requirements Hierarchy.....	16
Figure 5: DHS Transition Approaches.	18
Figure 6 DHS Requirements Gathering.....	20
Figure 7 We need to define problems, not propose solutions.	22
Figure 8 The Requirements Hierarchy (revisited).....	25
Figure 9 The Contents of an Operational Requirements Document.....	28
Figure 10 Potential Available Market Template.	41
Figure 11 Public-Private Partnership Benefits Analysis.....	45

Introduction

DHS is comprised of many organizational elements with a single purpose: to enable, support and expedite the mission-critical objectives of DHS' seven operating components and Directorates to protect our most valuable asset – our citizens. Transportation Security Administration (TSA); U.S. Customs and Border Protection (CBP); U.S. Secret Service (USSS); U.S. Citizenship and Immigration Service (USCIS); U.S. Immigration and Customs Enforcement (ICE); Federal Emergency Management Agency (FEMA); U.S. Coast Guard (USCG); and NPPD are the major organizations chartered within the Department to coordinate the transition of multiple agencies and programs into a single, integrated agency focused on protecting the American people and their homeland. The operating components and directorates work closely with, support and are supported by a large network of first responders at the state, local, tribal and territorial levels, along with the critical infrastructure and key resources (CIKR) owners and operators. These groups comprise DHS' stakeholder community and play critical roles in planning, preparedness, response and recovery efforts of DHS. The DHS stakeholders rely on the support of its many organizational elements to ensure mission success and address challenges confronting these stakeholders. Among the challenges facing DHS is how to gather and refine the needs and requirements of its various stakeholders, who represent a wide variety of mission spaces and operating environments, in a cost-effective and efficient manner.

The purpose of this guide is simple and straightforward: to enable the reader to effectively engage with the Department of Homeland Security in a simple and straightforward way. This resource will facilitate methods to articulate detailed operational requirements and define mission problems effectively, specifically those of the CIKR community. Readers will be able to better understand stakeholder interaction channels through various organizational elements and learn how to improve the communication of their needs and requirements to others in DHS, other Federal agencies, or the private sector.

Requirements form the cornerstone of understanding challenges faced in providing the capabilities necessary to complete mission critical objectives. Requirements further enhance one's ability to communicate those challenges to those who can best begin to address them. Often, we have heard expressions like "It all boils down to a lack of communication," or "We're not sure what you need," or "DHS has been difficult to work with because they really don't have a clear picture of their problems, needs or requirements." We can remedy this situation by implementing some fundamental practices in a disciplined manner so that requirements are both gathered and disseminated through the proper channels at the Department.

A well-written requirements document or articulation can be an effective tool to relay the needs of a given group in an easily understood format. Clear and consistent communications help to avoid the countless hours of time, money and other resources spent guessing about needs that are not clearly defined. Research conclusively shows that

the foremost reason programs or projects do not succeed is due to a lack of detailed requirements at the initiation of a program or project. Delays in bringing needed capabilities to the hands of those who need them most are not acceptable for those whose missions are critical to the protection of the American people and the critical infrastructure and key resources that support our everyday lives. Efforts invested early to develop a clear understanding of requirements pay dividends in the positive outcome of programs -- not to mention the savings in both time and money in corrective actions needed to get a program back on track (if it is even possible!).

We intend to make communication with DHS of your needs simple and easy. The Office of Infrastructure Protection (IP) along with the Science and Technology Directorate (S&T) work together to understand and address the needs and problems of the many CIKR communities. To that end, we have provided in this book an (a) introduction to working with DHS and its organizational elements responsible for assisting CIKR owners and operators and (b) an easy-to-follow template that will enable the generation and articulation of detailed operational requirements. We have also included several real-world examples of well-written operational requirements documents (ORDs) that show how complex challenges can be articulated. In the numerous appendices accompanying this book, you will find articles and briefings that provide additional context to the role that creating detailed operational requirements plays in effective product realization. It is our goal that this resource opens communication between DHS' stakeholders and the Department through positive interaction that leads to actions taken to address the needs and requirements of all stakeholders, whether they be direct DHS field agents, our nation's first responders or critical infrastructure and key resources owners and operators.

National Protection and Programs Directorate and the Office of Infrastructure Protection

The National Protection and Programs Directorate (NPPD) manages many aspects of the planning and preparedness functions of the Department. NPPD is comprised of a number of offices that effectively outreach and connect with several functional areas across the homeland security mission space important in the daily operations of the country. NPPD oversees the coordinated operational and policy functions of the Directorate's subcomponents – Cyber Security and Communications (CS&C), Infrastructure Protection (IP), Risk Management and Analysis (RMA), and the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program – in support of the Department's critical mission.

IP leads the coordinated national program to reduce risks to the nation's CIKR posed by acts of terrorism and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster or other emergency. This is a complex mission. CIKR range from the nation's electric power, food and drinking water to its national monuments, telecommunications and transportation systems, chemical facilities and much more. The vast majority of national CIKR is privately owned and operated, making public-private partnerships essential to protect CIKR and respond to events.

IP manages mission complexity by breaking it down into three broad areas: Identify and analyze threats and vulnerabilities; Coordinate nationally and locally through partnerships with both government and private sector entities that share information and resources; and Mitigate risk and effects (encompasses both readiness and incident response).

National Infrastructure Protection Plan and the Public-Private Partnership Model

The National Infrastructure Protection Plan (NIPP) was created to codify the nation's action plan to provide for CIKR resiliency, protection and preparedness (See Appendix A). The goal of the NIPP is to build a safe, more secure and more resilient America by enhancing protection of the nation's CIKR to prevent, deter, neutralize or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response and rapid recovery in the event of an attack, natural disaster or other emergency. The NIPP structure provides a foundation for strengthening disaster response and recovery. The CIKR Support Annex to the National Response Framework (NRF) provides a bridge between the NIPP "steady-state" processes for infrastructure protection and the NRF unified approach to domestic incident management. These documents provide the overarching doctrine that ensures full integration of the two vital homeland security mission areas – critical infrastructure protection and domestic incident management. The ways in which CIKR are interrelated creates additional challenges from cascading effects in the event of a disruption to sectors of CIKR.

Critical infrastructure protection is a shared responsibility among federal, state, local and tribal governments and the owners and operators of the nation's CIKR. Partnership between the public and private sectors is essential, in part because the private sector owns and operates approximately 85% of the nation's critical infrastructure while government agencies have access to critical threat information and each controls security programs, research and development and other resources that may be more effective if discussed and shared, as appropriate in a partnership setting.

The NIPP Partnership Model provides a forum through which the diverse community of infrastructure protection providers can collaborate and share information to discuss requirements identification, planning and policy coordination. This unique set of infrastructure protection providers encompasses groups of CIKR owners and operators along with government officials at all levels. See Figure 1 for the structure of the NIPP Partnership Model.

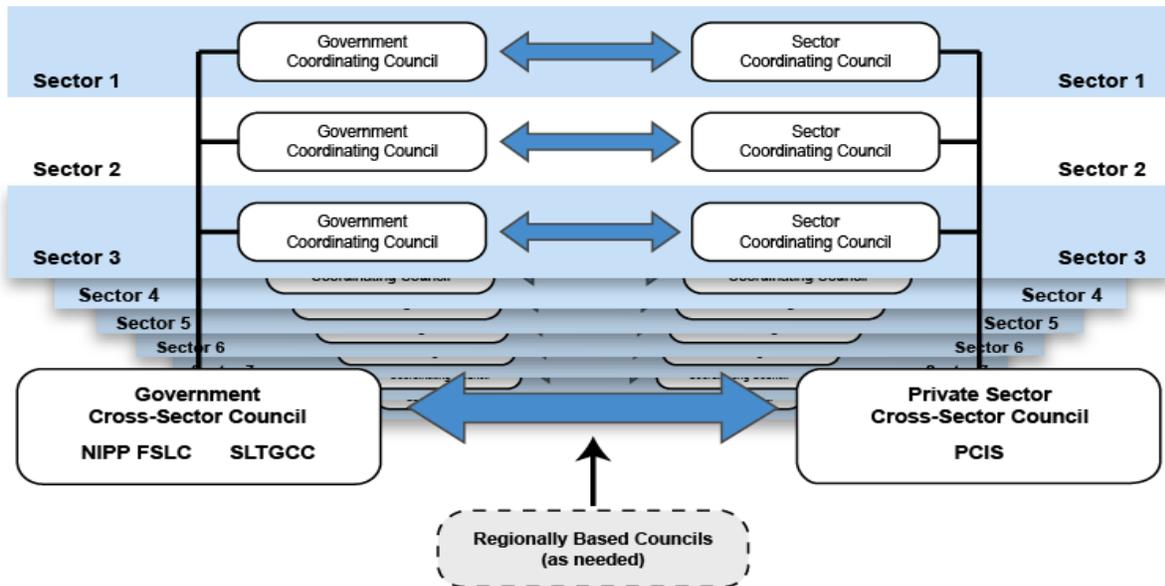


Figure 1. The NIPP Partnership Model is a collaborative forum for Government and Private Sector entities at Federal, State, Local and Tribal levels responsible for infrastructure protection can share information and ideas on requirements. This model is duplicated for each Sector Coordinating Council (SCC).

Under the NIPP, a Sector-Specific Agency (SSAs) is the assigned federal agency to lead a collaborative process for infrastructure protection for each of the eighteen sectors. The comprehensive NIPP framework allows IP to provide the cross-sector coordination and collaboration needed to set national priorities, goals and requirements for effective allocation of resources. More importantly, the NIPP framework integrates a broad range of CIKR public and private protection activities.

The SSAs provide guidance about the NIPP framework to state, territorial, tribal and local homeland security agencies and personnel. They coordinate NIPP implementation within the sector, which involves developing and sustaining partnerships and information-sharing processes, as well as assisting with contingency planning and incident management.

IP serves as the SSA for six of the eighteen CIKR sectors. IP works closely with SSAs of the other twelve CIKR sectors to implement the NIPP. This frequently involves addressing cross-sector vulnerabilities and working to achieve cross-sector program efficiencies. The sectors for which IP serves as the SSA are italicized:

Agriculture and Food	Defense Industrial Base	National Monuments &
Banking and Finance	<i>Emergency Services</i>	Icons
<i>Chemical</i>	Energy	<i>Nuclear Reactors,</i>
<i>Commercial Facilities</i>	Government Facilities	<i>Materials and Waste</i>
Communications	Healthcare and Public	Postal and Shipping
<i>Critical Manufacturing</i>	Health	Transportation Systems
<i>Dams</i>	Information Technology	Water

An important facet of these sectors is the creation of Cross-Sector Councils. The many ways in which CIKR are interrelated creates additional challenges from cascading effects in the event of a disruption to various CIKR sectors. The collaborative nature of Cross-Sector Councils benefits gathering not only information on those cascading effects and interdependencies, but also provides insight into commonly shared requirements that may be addressed by similar solutions. This information provides significant details to solution developers into the detailed problem description as well as opens opportunities for the deployment of multi-use technologies and a reduction in redundant programs that solve similar problems.

Working through these sectors, IP assists NIPP stakeholders in identification and articulation of strategic R&D needs. IP oversees the collection, distribution and prioritization of sector requirements for all eighteen sectors. IP also facilitates the coordination of addressing the needs of these stakeholders with other Department organizational elements to address identified capability gaps. An analysis of the stakeholders of these CIKR markets shows that there are many CIKR owners and operators who need to be able to engage with DHS to convey their requirements. These sectors also represent large user groups that often require widely distributed products and services to meet their needs nation-wide. See Figure 2 for a breakdown of the eighteen sectors and their component stakeholders.

These sectors play a critical role in the understanding of capability gaps and requirements experienced by the CIKR owners and operators. This direct interaction between the Government Coordinating Council (GCC) and Sector Coordinating Council (SCC) provides opportunities for these groups to develop a common understanding of current challenges facing the sectors. This partnership model allows for “bottoms-up requirements gathering” that can be shared through the well-defined process and reach those groups able to act upon the gathered information. IP has a close relationship with several organizational elements throughout the Department to not only find common requirements and capability gaps, but also to work with those best able to develop and deploy technological solutions to those in need

Critical Infrastructure Key Resources (CIKR)

Agriculture and Food	Defense Industrial Base	Energy	Public Health and Healthcare	National Monuments and Icons	Banking and Finance	Water	Chemical	Commercial facilities	Emergency Services	Materials, Reactors and	Telecommunications	Critical Manufacturing	Postal and Shipping Services	Transportation	Information Technology
Food Retail _\$_; _ Units	Defense Contractors _\$_; _ Units	Coal mining operations _\$_; _ Units	Public/University hospitals _\$_; _ Units	Guided tour services _\$_; _ Units	Credit lending institutions _\$_; _ Units	Public utilities _\$_; _ Units	Inorganic chemical production _\$_; _ Units	Hotels _\$_; _ Units	Fire Departments _\$_; _ Units	Electric utilities _\$_; _ Units	Telephone/Cellular services _\$_; _ Units	Iron and Steel mills _\$_; _ Units	United States Postal Service _\$_; _ Units	AMTRAK _\$_; _ Units	Hardware providers _\$_; _ Units
Farm Equipment _\$_; _ Units	Industry analysis _\$_; _ Units	Coal power plants _\$_; _ Units	Private/For Profit hospitals _\$_; _ Units	Travel services _\$_; _ Units	Commercial banking _\$_; _ Units	Desalinization plants _\$_; _ Units	Organic industrial production _\$_; _ Units	Shopping centers _\$_; _ Units	Law enforcement agencies _\$_; _ Units	Reactor and associated materials _\$_; _ Units	Satellite data transmission _\$_; _ Units	Aluminum production and processing _\$_; _ Units	High volume document and parcel shipping _\$_; _ Units	Commuter rail _\$_; _ Units	IT Conglomerates _\$_; _ Units
Meat/Poultry Processing _\$_; _ Units	Think tanks/research institutions _\$_; _ Units	Coal equipment manufacturers _\$_; _ Units	Clinics _\$_; _ Units	Lodging/Hotel _\$_; _ Units	Private equity _\$_; _ Units	Treatment plants _\$_; _ Units	Ceramics _\$_; _ Units	Stadiums and sport arenas _\$_; _ Units	Search and rescue teams _\$_; _ Units	University and educational institutions _\$_; _ Units	Broadcasting entities _\$_; _ Units	Nonferrous metal production and processing _\$_; _ Units	Container shipping services _\$_; _ Units	Intracity rail services _\$_; _ Units	Semiconductor production _\$_; _ Units
Food Processing _\$_; _ Units	University partnership programs _\$_; _ Units	Hydroelectric _\$_; _ Units	Private medical practices _\$_; _ Units	Guest services/tourist hospitality _\$_; _ Units	Consumer banking _\$_; _ Units	Equipment manufacturers _\$_; _ Units	Petrochemicals _\$_; _ Units	Schools _\$_; _ Units	Ambulance companies _\$_; _ Units	Control systems _\$_; _ Units	Broadcast equipment manufacturing _\$_; _ Units	Engine, Turbine and Power transmission _\$_; _ Units	Marine shipping _\$_; _ Units	Commercial airline _\$_; _ Units	Electronics manufacture _\$_; _ Units
Dairy Processing _\$_; _ Units	National laboratories _\$_; _ Units	Dam operations _\$_; _ Units	Medical laboratories _\$_; _ Units	People moving services _\$_; _ Units	Building societies/Private banks _\$_; _ Units	Pipe and water control device manufacturers _\$_; _ Units	Agrochemicals _\$_; _ Units	Commercial office buildings _\$_; _ Units	Mountain/Cave/ Mine rescue teams _\$_; _ Units	Nuclear safety systems _\$_; _ Units	Radio equipment manufacturing _\$_; _ Units	Marine shipping _\$_; _ Units	Private air services _\$_; _ Units	IT services _\$_; _ Units	Server and network hardware _\$_; _ Units
Dairy Farms _\$_; _ Units		Wind power _\$_; _ Units	Pharmaceutical _\$_; _ Units	Queuing equipment makers _\$_; _ Units	Merchant banks _\$_; _ Units		Polymers _\$_; _ Units	Museums _\$_; _ Units	Other technical rescue teams _\$_; _ Units	Waste disposal services _\$_; _ Units	Electrical equipment manufacturing _\$_; _ Units	Trucking industry _\$_; _ Units	Cruise lines _\$_; _ Units	Subway systems _\$_; _ Units	Display/digital TV _\$_; _ Units
Ranching _\$_; _ Units		Solar power _\$_; _ Units	Health insurance _\$_; _ Units	Private security _\$_; _ Units	Global financial services firms _\$_; _ Units		Elastomer production _\$_; _ Units	Zoos and Aquariums _\$_; _ Units	Bomb disposal units _\$_; _ Units	Uranium processors _\$_; _ Units	Motor Vehicle manufacturing _\$_; _ Units	Airborne shipping _\$_; _ Units	Distribution services _\$_; _ Units	Long-haul maritime shipping _\$_; _ Units	Software production _\$_; _ Units
Organic Farming/Sustainable Agriculture _\$_; _ Units		Public utilities companies _\$_; _ Units	Medical material providers _\$_; _ Units		Community development _\$_; _ Units		Oleochemicals _\$_; _ Units	Public Libraries _\$_; _ Units	Blood/Organ transplant supply _\$_; _ Units	Protective garment manufacturers _\$_; _ Units	High speed data transmission _\$_; _ Units	Aerospace product & parts manufacturing _\$_; _ Units	Trucking _\$_; _ Units	Freight rail service _\$_; _ Units	Information security _\$_; _ Units
Traditional Planting _\$_; _ Units		Oil companies _\$_; _ Units	Medical equipment manufacturers _\$_; _ Units		Community banks _\$_; _ Units		Explosives _\$_; _ Units	Amusement parks _\$_; _ Units	Amateur radio emergency comms _\$_; _ Units	Internet service providers _\$_; _ Units	Internet service providers _\$_; _ Units	Railroad rolling stock _\$_; _ Units	Bus services _\$_; _ Units	Automobile travel _\$_; _ Units	Semiconductor equipment _\$_; _ Units
Commercial fishing _\$_; _ Units			Medical technology manufacturers _\$_; _ Units		Savings and Loans _\$_; _ Units		Fragrance production _\$_; _ Units		Public utility protection providers _\$_; _ Units	Print media _\$_; _ Units	Internet technology providers _\$_; _ Units	Other Transportation equipment _\$_; _ Units	Freight rail service _\$_; _ Units	Roads, Highways, bridges and tunnels _\$_; _ Units	
			Biotechnology _\$_; _ Units		Credit unions _\$_; _ Units		Chemical wholesale _\$_; _ Units		Emergency Road services _\$_; _ Units	Emergency Social services _\$_; _ Units					
					Insurance companies _\$_; _ Units		Exotic chemicals _\$_; _ Units		Emergency response teams _\$_; _ Units	Community emergency response teams _\$_; _ Units					
					Insurance brokerages _\$_; _ Units				Disaster relief _\$_; _ Units	Famine relief teams _\$_; _ Units					
					Reinsurance companies _\$_; _ Units				Poison Control units _\$_; _ Units	Animal control teams _\$_; _ Units					
					Stock brokerages _\$_; _ Units				Wildlife services _\$_; _ Units						
					Capital market banks _\$_; _ Units										
					Custody services _\$_; _ Units										
					Angel investment _\$_; _ Units										
					Venture capital _\$_; _ Units										



Homeland Security

DHS Science and Technology Directorate

Advances in science and technology continue to spur the development of new and innovative products focused on the homeland security market. As this marketplace expands, it becomes increasingly important for homeland security personnel to assist in guiding product development to match their various needs. Delivering these customer-driven products and technologies is a primary objective for DHS.

For many organizational elements within DHS, their primary focus is to assist in policy management, preparedness planning and crisis mitigation efforts. These support functions are critical to component field agents, first responders and infrastructure protection personnel. As Department stakeholders perform their missions, they inevitably are faced with situations where their current capabilities are not sufficient to carry out their objectives. Ever-changing threat dynamics often require new, innovative technology-based solutions in order to prevent or mitigate the potential effects of current and future dangers, not to mention the numerous challenges faced by these groups on a daily basis that are integral to providing security for all citizens. Chief among the organizational elements charged with delivering new products and capabilities is the DHS Science and Technology Directorate (S&T). DHS S&T is unique in that it is the organizational element within the Department whose primary mission is to provide Department stakeholders with the technologies, products, and services needed in order to perform their objectives.

DHS S&T is organized into several divisions to address stakeholder requirements in the fields of basic research, high-risk/high-reward innovation projects and product transition activities that serve to get products into the hands of stakeholders to enhance their mission capabilities. In today's dynamic homeland security environment, delivering customer-driven products and technologies is a primary objective for DHS. DHS S&T manages DHS' diverse group of operating components and supporting elements whose missions address a wide variety of terrorist and natural threats to our homeland.

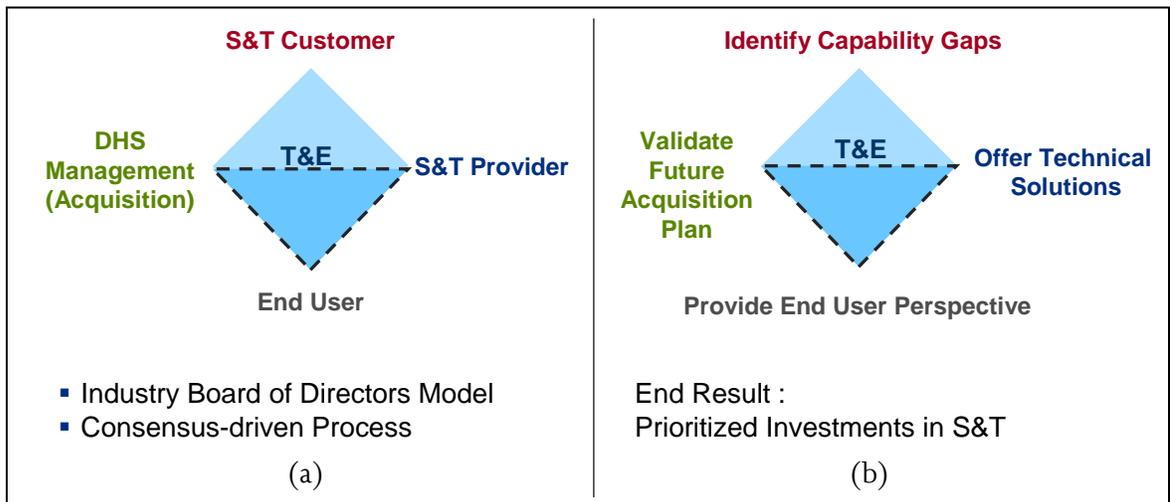
DHS S&T works to understand, document and offer solutions to current and anticipated threats faced by these stakeholders; our "customers" (and our "customers' customers" (first responders and CIKR owners and operators). DHS S&T, through the Capstone Integrated Product Team (IPT) process ensures that quality, efficacious products are developed in close alignment with detailed customer needs. The Capstone IPT process represents the requirements-driven, output-oriented portion of DHS' technology development investments geared toward providing DHS stakeholders with the necessary tools to protect America's most valuable assets – its people.

Capstone Integrated Product Teams

The Capstone Integrated Product Teams (IPTs) are chartered to ensure that technologies and products are engineered and integrated into systems aligned to the needs of DHS customers. Consistent with the Homeland Security act of 2002, Capstone IPTs establish a lean and agile world-class S&T management team that delivers the technological advantage necessary to ensure DHS agency mission success. The Capstone IPT process is the framework used to determine whether developed capabilities meet operational needs, analyzes gaps in strategic needs and capabilities, develops operational requirements, and develops programs and projects to close capability gaps and expand mission competencies. This process is a customer-led forum through which the identification of functional capability gaps and the prioritization of these gaps across the Department are formalized. The Capstone IPTs manage the research and development efforts of DHS S&T and enable the proper allocation of resources to the highest priority needs established by the DHS operating components.

The Capstone IPT process is a model that requires the participation and input from several DHS stakeholders. This collaborative effort centers on the principle that the customer is “the focus” of this process. The product and technology outputs of the Capstone IPT process are customer-requirements-driven from start to finish. The customer is involved throughout the process to ensure that they receive products and technologies specifically aligned to their detailed operating requirements. Ultimately, our customers receive quality products that effectively deliver the necessary, mission-critical capabilities to secure our nation.

Led by the DHS S&T customer, Capstone IPTs bring together DHS S&T division heads, acquisition partners and end-users (operating components, field agents and supporting first responders – customers of DHS) involved in the research, development, testing and evaluation (RDT&E) and acquisition activities. Working together, the Capstone IPT members identify, evaluate and prioritize the operational requirements necessary to complete missions successfully. Based on information gained from Capstone IPT meetings, DHS S&T providers assess the technological and system development of products that will ultimately be deployed into the field. Figure 2 shows the general organization of a Capstone IPT. The figure also contains the specific members of the Infrastructure Protection IPT. The Office of Infrastructure Protection chairs the Infrastructure Protection IPT on behalf of the Sector Coordinating Councils. The formalization of efforts between the Office of Infrastructure Protection and the Capstone IPT process at an early stage allows key stakeholders to identify and address critical capability gaps.



Infrastructure Protection

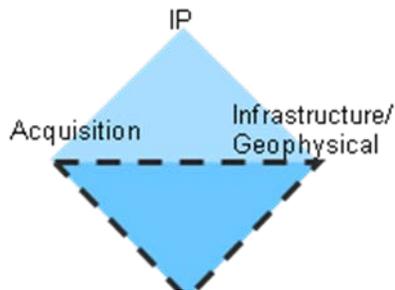


Figure 2. (a) This diagram shows the structure of the Capstone IPT model with (b) the models' output functions carried out by each IPT member and (c) the organization of the Infrastructure Protection IPT.

The Capstone IPTs are structured to focus on functional, department-level requirements and deal with programmatic and technology issues within the six DHS S&T divisions: Explosives (EXD), Chemical/Biological (CBD), Command Control and Interoperability (C2I), Borders and Maritime Security (BMD), Human Factors (HFD) and Infrastructure and Geophysical (IGD). Capstone IPTs have been created across thirteen major homeland security core functional areas: Information Sharing/Management, Cyber Security, People Screening, Border Security, Chemical/Biological Defense, Maritime Security, Counter-Improvised Explosive Devices, Transportation Security, Incident Management, Interoperability, Cargo Security, Infrastructure Protection, and First Responders.

Each Capstone IPT is chaired or co-chaired by senior leadership from a DHS operating component or federal organizational element with corresponding needs within a specific functional area. The chair/co-chair, representing the end-users of a delivered capability, engage throughout the process to identify, define and prioritize current and future requirements and ensure that planned technology and/or product transitions and acquisition programs, commercialization efforts and standards development are optimally suited to their operational requirements. Operating components, field agents, first responders and other non-captive end-users with an interest in the core functional areas of

a Capstone IPT are welcome to participate and contribute throughout the Capstone IPT process. See Figure 3 for the captive members for each IPT.

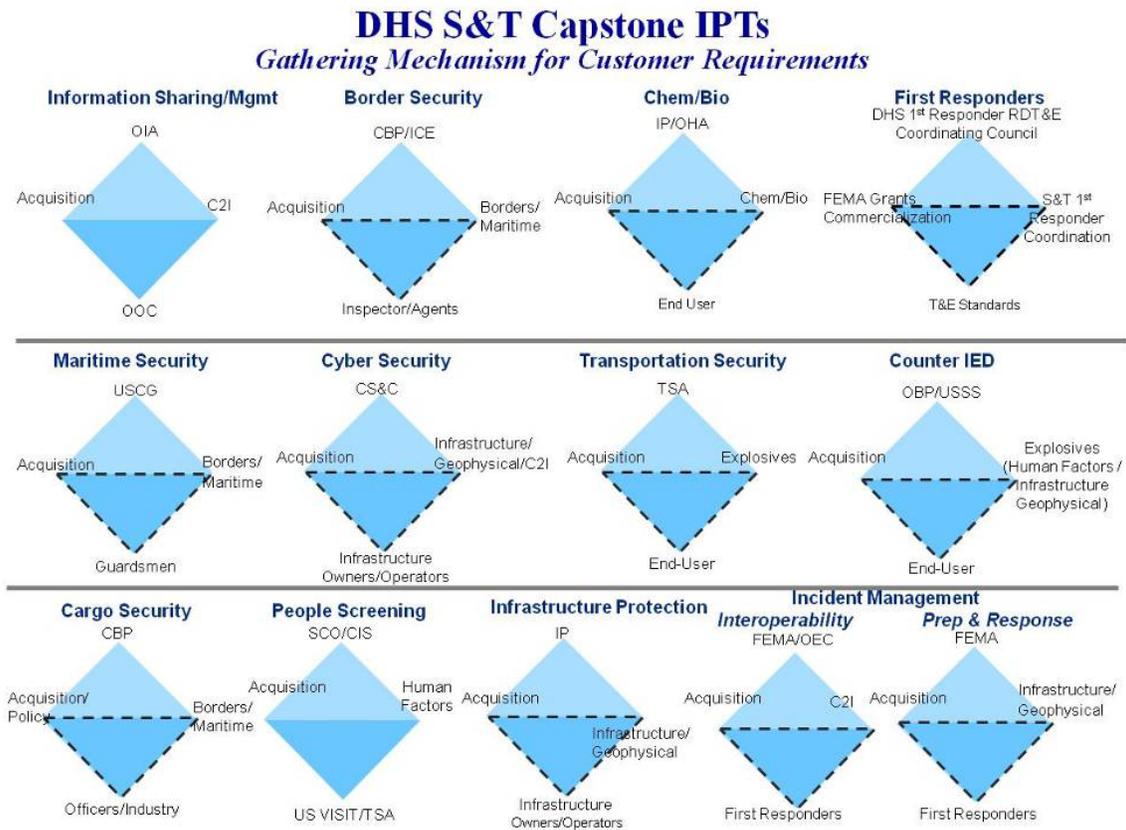


Figure 3. This diagram shows the thirteen Capstone IPTs, the DHS operating component, DHS end-user(s), the S&T Division technical provider, and, when applicable, the Acquisition conducted by DHS management.

Capstone IPTs purposefully cover very broad core functional areas. This broad focus aids in reducing the duplication of efforts geared toward various operating components of DHS. It is often the case that a given capability gap is experienced by numerous operating components and stakeholders simultaneously and can thus share in the capabilities provided. Technology development is functionally aligned to allow technologies to be used in support of multiple operating components and customer sets within DHS. The effective management and communication of capability gaps ensures that similar efforts are either combined or developed in concert so that required capabilities are provided to as many stakeholders sharing similar capability gaps, reducing overall technology development costs and accelerating the time-to-market for certain capabilities.

The mission of the Infrastructure/Geophysical Division (IGD) is to improve the Nation’s preparedness and response to natural and man-made threats by developing technology to enhance situational awareness, emergency response capabilities, and critical infrastructure protection. The Infrastructure/Geophysical Division supports

Federal, State, local, tribal, territorial, and private sector for all-hazards events that impact both the U.S. population and critical infrastructure.

IGD conducts research and development (R&D) activities for the 18 Critical Infrastructure and Key Resource (CIKR) Sectors identified in the NIPP. The NIPP provides the overarching approach for integrating the Nation's many CIKR protection initiatives into a single national effort.

- IGD receives the highest priority capability gaps from the 18 CIKR sectors as identified in the Sector Annual Reports. IGD works with the Office of Infrastructure Protection, R&D Project Office to analyze, organize and prioritize the gaps.
- IGD gathers customer requirements through the Capstone Integrated Product Team (IPT) process, which is chaired by the Office of Infrastructure Protection. The Infrastructure Protection Capstone IPT is comprised of staff from the Office of Infrastructure Protection, IGD, as well as the R&D provider, and the ultimate end users (infrastructure owners and operators). The Capstone IPT is customer-driven and user oriented, and provides a mechanism by which owners and operators gain visibility into the R&D development life cycle from inception to completion.
- IGD and IP have formed the Committee on Requirements (CoRe), which focuses on reviewing unfunded and new gaps submitted by the sectors and developing recommendations for a way ahead with these gaps.

Capability Gaps and Enabling Homeland Capabilities

Capstone IPTs generate several outputs that guide the development and fielding of technologies and systems for DHS' stakeholders. The primary role of the Capstone IPTs is to conduct strategic needs analyses to determine and prioritize the capability gaps that exist within a given functional area. Capability gaps are broad descriptions of department level identified mission needs that are not met given current products and/or standards. Capability gaps catalog opportunities for enhanced mission effectiveness or address deficiencies in national capability. Capability gaps often start with "We need to be able to do..." statements that identify mission needs rather than suggested solutions. See Figure 4 for the requirements hierarchy diagram.

Requirements Hierarchy (TSA example)

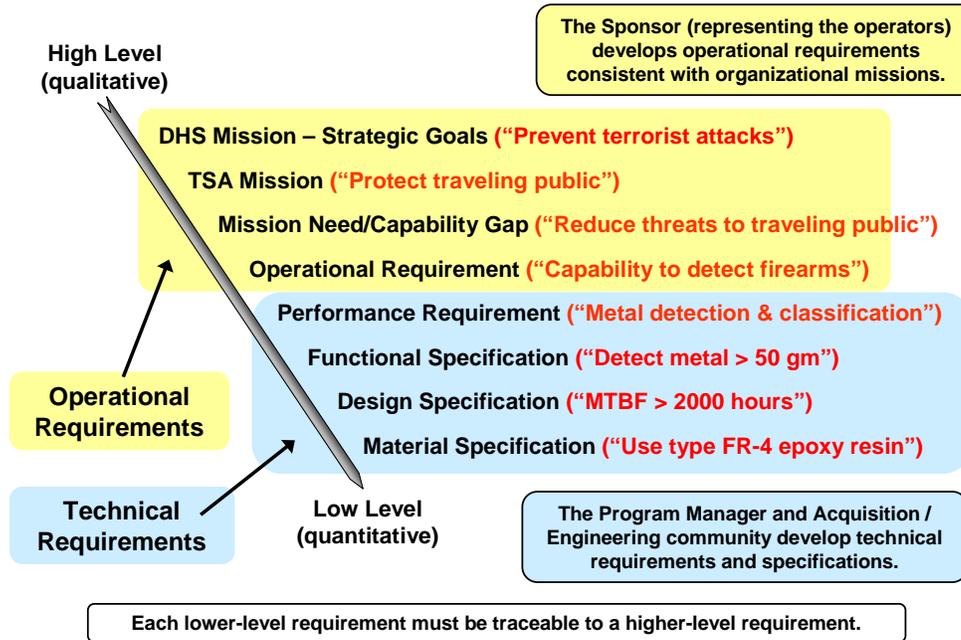


Figure 4. This “requirements hierarchy” shows the evolution of requirements from a high-level macro set of operational requirements to a low-level micro set of technical requirements. Note that each lower level requirement stems directly from its higher requirement so that all requirements are traceable to the overall DHS Mission.

Led by their IPT Chairs/Co-chairs, Capstone IPTs are responsible for the analysis, identification, and prioritization of their capability gaps. Capability gaps can come in several forms. Some gaps may appear in the form of modified personnel and resource allocation, training, standards, plans/protocols/procedures, resources, technology, systems, etc. For those capability gaps requiring technology-based solutions, a grouping of technology components is identified by DHS S&T to address the various needs delineated in the capability gaps. These grouped technology solutions, or Enabling Homeland Capabilities (EHCs), collectively deliver new gap closing capabilities to the customers. EHCs focus on the technology pieces that develop, mature and deliver to DHS acquisition programs, are commercialized, or are validated as a standard within a three-year period or less. DHS S&T develops EHCs that contain quantifiable metrics that allow for effective management of development progress. These metrics define how the EHC will address/close the related capability gap, the cost and schedule over the life of the EHC, identify the specific S&T efforts addressing the EHC and endorsements, and recommendation of proposed EHCs and corresponding deliverables by the relevant Capstone IPT. EHCs enable customers and DHS S&T engineers to focus on discussions related more broadly to overall capability needs and operational requirements rather than discussions simply about potential solutions to problems.

Project-IPTs: Managing the Day-to-Day Development of Capabilities

The Capstone IPT process enables the DHS S&T divisions to interact regularly with their customers to address capability gaps. These capability gaps in many ways are just the beginning. Additional detail about their requirements must be gathered to enable the cost-effective and efficient development of a technology or product. In order to achieve greater insight into the details that comprise each Capstone IPT, Project-IPTs are created to manage specific project areas within a functional area. While Capstone IPT meetings occur at regular intervals throughout the year, Project-IPTs are created to manage closing capability gaps gathered from the larger Capstone IPT on a daily basis. For example, Border Officer Tools and Safety, and Container Security are Project-IPTs for the Border Security and Cargo Security Capstone IPTs, respectively. Project-IPTs consist of several DHS S&T subject matter experts who are responsible for clarifying the capability gaps derived from the Capstone IPTs and for gathering additional insight into operational requirements with the customers for the overall capability enhancement that is necessary. These requirements assist in decomposing a high-level capability gap into the individual components that may comprise a potential solution. Through this process the grouping of individual technologies into an integrated system creates the overall EHC.

The Project-IPTs work closely with DHS customers to develop a robust understanding of customer needs, through an operational requirements document (ORD), to define clearly the specific requirements that must be met in order for a technological solution to address a given problem. Development of detailed ORDs further enhances the direction in which technology and product development efforts progress and further reduces duplication of effort across various Project and Capstone IPTs. These subject matter experts are also involved in conducting market surveys, analyses of alternatives and other functions related to technology and product evaluation ensuring that developed capabilities are aligned to customers' needs. Additionally, Project-IPTs serve a critical role in integrating developed capabilities into EHCs and fully deployable systems that provide customers with enhanced mission capabilities. All DHS agencies are responsible for integrating and fielding the technology deliverables into operational systems scheduled for delivery to their operating component.

Management – DHS Leadership and DHS S&T

The Capstone IPTs prioritize EHC proposals that respond to customer capability requirements. DHS leadership has a critical role in determining Capstone IPT funding levels and investments once prioritized EHCs are identified. Once approved, budgets are submitted, solicitations may be issued, pre-award technical reviews are conducted, and commercialization efforts are considered. DHS leadership conducts reviews of current EHCs every six months to ensure that EHCs meet cost objectives and that technical development is progressing along milestones. DHS leadership also reviews new EHCs and continually reviews on-going EHCs in order to make informed decisions regarding continued funding of programs.

The Transition Office manages the process to develop and deliver required technologies/products as defined in the EHCs. Working with its customer requirements, DHS S&T proposes the technology-based solutions approved EHCs to the Capstone IPTs. By understanding the needs and requirements of its customers, DHS S&T identifies the programs that are ineffective/insufficient in meeting the EHC expectations and offer technical solutions to address the stated requirements. DHS S&T works to conduct market and technology scans to find technology-based solutions that can be developed matured and delivered to DHS acquisition programs, commercialized or validated as a standard within a three-year period.

There are several ways products can transition “out of the lab” into fully developed, widely distributed products for the large customer communities. Figure 4 identifies possible transition paths to deliver products to customers. DHS S&T may recommend available commercial-of-the-shelf (COTS) products or other non-S&T alternatives in lieu of developing a new DHS S&T solution. DHS S&T also reviews private sector responses to solicitations for capabilities that can be readily addressed with COTS products. Once development plans are approved, DHS S&T engages and involves the customer via technology demonstrations and experimentation to ensure adequate customer feedback throughout the development life cycle. DHS S&T manages costs, schedules and technical performance of programs under the oversight of the Capstone IPT. The Director of Transition chairs monthly status meetings that allow technology execution problems to be discussed and resolved in a timely and effective manner.

Transition Approaches

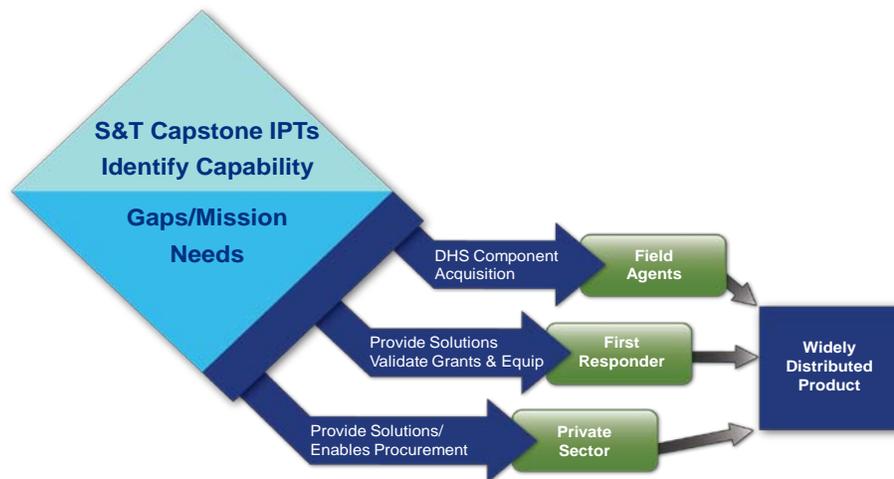


Figure 5. DHS has three major methods to transition products to end-users. DHS field agents are captive end-users of the Capstone IPT process while the First Responder community is typically able to select its own solutions. Capabilities are also transitioned to CIKR owners and operators in the private sector. All newly proposed DHS programs must now identify technologies/products already in development in the private sector that are aligned with end-user requirements that enable users to make informed purchasing decisions.

Technology Transition Agreements (TTAs)

Technology Transition Agreements (TTAs) represent a good-faith contract between the DHS S&T developer and the DHS customer. The TTA is negotiated and signed at the product level by those communities responsible for a delivering or advocating a specific product or technology. As a consensus agreement, the TTA is signed by all of the stakeholders responsible for the technology/product in order for continued funding. This good faith agreement determines the specific exit criteria that must be demonstrated in order for the “hand off” of the technology/product to the customer. In the case of the Infrastructure Protection IPT, the Office of Infrastructure Protection again serves as the representation to the Capstone IPT process on behalf of CIKR owners and operators.

The TTA provides a detailed description of the deliverable promised by the DHS S&T program managers. The customer program manager certifies that the need for the product or technology is consistent with the needs/requirements as defined by their operating component, and the requirements or acquisition agents state their commitment to integrate the successfully demonstrated technology/product or into an identified and funded acquisition program. The TTA ensures that all parties explicitly understand the deliverable is aligned to customer needs and that a funding source is available and aligned with the customer’s needs. If any problems are identified by DHS S&T, customer agency or acquisition offices, all parties are informed and decisions are made regarding continued funding. Once the TTA has been signed the next step is to move forward with product development and eventual product deployment to the customers.

Using Technology to Give Boots on the Ground a Voice

Traditional communication through e-mail and phone calls has proven insufficient in gathering and compiling input from the sheer number of stakeholders responsible for providing protection to our homeland. There remains room for improvement in gathering requirements from the many different stakeholders across the country. In many ways, the private sector possesses much more reliable information than is seen from DHS’ previous, seemingly disjointed approach. Continued work through the Capstone IPTs and DHS’ Requirements Development Initiative training materials will reduce the inefficiency of DHS personnel by providing a common point of entry for end-user representatives and perspectives.

Just as needed is deployable technology to create a Community of Practitioners (CoP). DoD has invested in these kinds of technologies to enable reaching not only the millions of first responders nation-wide but also other customers and potentially authorized stakeholders (other federal agencies, private sector, venture community, etc). Advanced technologies like the “Semantic Web 3.0” will aid in the communal and open development of capability gaps, ORDs, potential available market sizing/applications, etc. all at the benefit of the American taxpayer, Government and private sector. We are finalizing plans to initiate a pilot program to harness these technologies to engage various user communities to enable broad-based development of widely accepted operational

requirements. Figure 6 shows graphically the evolving processes used for developing requirements at DHS S&T.

Evolution of Change: DHS Providing Better Information about its Needs

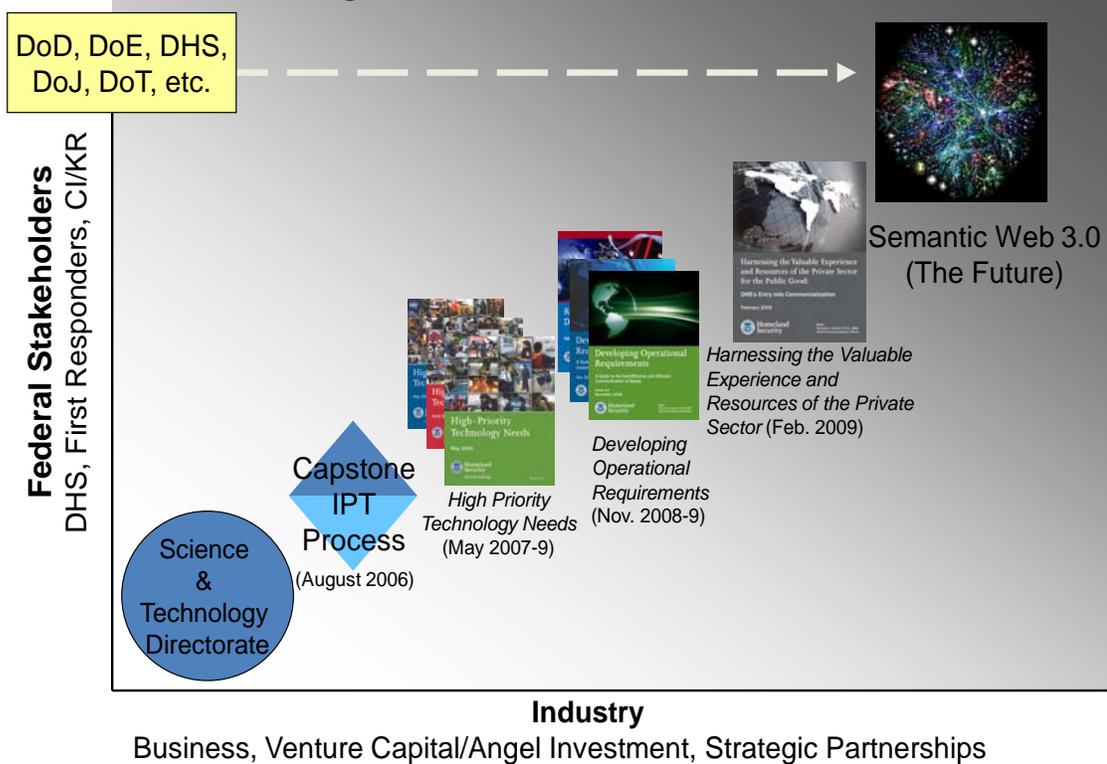


Figure 6. DHS has progressed in the way that it reaches out to its stakeholders to learn about their needs. Advanced social networking technologies have the potential to greatly enhance communications and understanding of needs.

It is clear that DHS S&T needs to lead the development of an easy-to-use technology to generate a CoP for its customer communities. The vast majority of the millions of DHS’ stakeholders need to be invited to play an active role in creating, editing and prioritizing detailed operational requirements to be used by DHS in order to provide (or facilitate through its commercialization efforts) solutions for the stakeholders communities. This approach enables both a “bottom-up” and “top-down” view of detailed user requirements – avoiding the age-old discussion of whether a “bottom-up” or “top-down” approach is superior. New social networking technologies have opened new opportunities that allow communication to flow and leverage the merit of both approaches.

DHS S&T plans to create a set of detailed operational requirements of a system prototype that, in general:

- Effectively leverages advanced social networking and information sharing (utilizing semantic architecture and TRL management) using genuine DHS scenarios such as developing/editing ORDs, all at the benefit of taxpayers in an open and transparent way for all to participate easily
- Expandable to millions of users in the First Responder, CIKR, and potential solution providers (private sector) communities
- Expandable to include vital interagency partners like DoE, DoD, and National Laboratories for gauging potential users and potential available market sizing
- Expandable to include Venture Capital, Angel Investor and Corporate Investor Communities, if desired and/or required

Product Realization through Requirements Articulation

If you think about it, we can point to many examples in both our professional and private lives where the lack of communication or unclear terminology has created misunderstandings, problems and a myriad other issues. Effective communication is critical in the cost-effective and efficient interactions between various parties seeking a mutually beneficial relationship or partnership.

At every step of product development, it is critical to understand and meet user needs. Developing requirements to guide effective product development is not a trivial effort; but with proper planning, dedication and communication, successful product development can yield measurable positive results and provide DHS operating components, first responders, CIKR owners and operators and other stakeholders with resources necessary to carry out their mission-critical objectives to protect our nation.

The initial phase of product realization is a mission needs assessment. This assessment should be conducted in relation to the overall mission for an organization. This exercise identifies capabilities needed to perform required functions, highlights deficiencies in a functional capability and documents the results of the analysis. Some of these capabilities may already be addressable with existing products, systems or services currently accessible by an organization. Analysis may also show that material solutions may not be necessary to solve a problem, as issues may be resolved through resource redistribution, staffing adjustments, standards development and other actions that do not require the fielding of new technologies. Additionally, a mission needs assessment serves to identify deficiencies in current and projected capabilities. In the event that current products are not able to address a particular capability; a capability gap exists. Briefly, capability gaps are defined by the difference between current operational capabilities and those necessary capabilities needed to perform mission-critical objectives that remain unsatisfied. Capability gaps must be listed in terms of an overall need to perform a specific task and should avoid explaining how that task should be achieved. Capability

gaps that are discovered and articulated from a mission needs assessment form the foundation of the Capstone IPT process See Appendix K for further reading.

For example, faced with the problem of potential intruders to a sensitive facility, we might define the requirement as “build a wall,” whereas the real requirement is “detect, thwart, and capture intruders.” Our wall might “thwart” intruders (or might not, if they’re adept at tunneling), but it would not detect them or facilitate their capture. In short, the solution would not solve the problem.

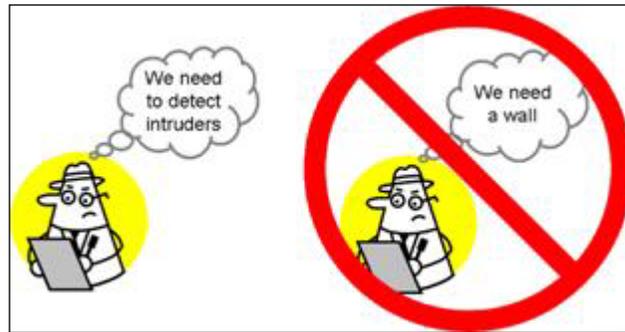


Figure 7. We need to define problems, not propose solutions.

The robust capability gap to “detect, thwart, and capture intruders” includes no preconceived solutions and prompts us to analyze alternative conceptual solutions and choose the best.

One way to ensure that we are defining a problem, rather than a solution, is to begin the statement of the requirement with the phrase “we need the capability to ...” It’s nearly impossible to complete this sentence with a solution (“a wall”), and much easier to complete the sentence with a problem (“capability to detect intruders”). Capability gaps and requirements should address what a system should do, rather than how to do it. This approach is sometimes called capability-based planning. It is a very simple, yet powerful concept.

Properly defining clear and concise capability gaps is a necessary first step in product realization. This high-level understanding of a problem is a key part in the communication of needs. One may find that capability gaps are oftentimes common for multiple cross-sections of DHS operating components and supporting elements such as the first responder community and private sector critical infrastructure owner/operators. Discovering these commonalities is a fundamental aspect of the DHS S&T Capstone IPT Process, which seeks to reduce duplication of efforts and expedite product transition. See Appendix C for further information.

Why Requirements?

Capstone IPTs generate several outputs that guide the development and fielding of products, services and systems for DHS operating components, primary in the form of

capability gaps that exist within a particular functional area. These broad descriptions of department-level identified mission needs that are not met given current products and/or standards catalog opportunities for enhanced mission effectiveness or address deficiencies in national capability. However, capability gaps are just the first step in providing solutions to mission-critical needs. Operational requirements bring detailed information to support the capability gaps and define actionable information through detailed definitions of the problems, which need to be further delineated into technical requirements.

A requirement is an attribute of a product, service or system necessary to produce an outcome(s) that satisfies the needs of a person, group or organization. Requirements therefore define “the problem.” In contrast, “the solution” is defined by technical *specifications*.

Defining requirements is the process of determining what to make before making it. Requirements definition creates a method in which appropriate decisions about product or system functionality and performance can be made before investing the time and money to develop it. Understanding requirements early removes a great deal of guesswork in the planning stages and helps to ensure that the end-users and product developers are “on the same page.”

Requirements provide criteria against which solutions can be tested and evaluated. They offer detailed metrics that can be used to objectively measure a possible solution’s effectiveness, ensuring informed purchasing decisions on products, systems or services that achieve the stated operational goals. A detailed requirements analysis can uncover hidden requirements as well as discover common problems across programs and various DHS operating components. Detailed operational requirements will guide product development so that solutions’ specifications actively solve the stated problems.

We could save ourselves a lot of work if we jump straight to “the solution” without defining “the problem.” Why don’t we do that? Because if we take that shortcut we are likely to find that our solution may not be the best choice among possible alternatives or, even worse, we’re likely to find that our “solution” doesn’t even solve the problem!

Defining requirements and adhering to developing solutions to address those needs is often referred to as “requirements-pull.” In this situation, user requirements drive product development and guide the path forward as the requirements dictate. This is a powerful circumstance in which fulfilling requirements becomes the central focus of product development and no possible solution is disregarded given it facilitates addressing the stated operational requirements.

At the other extreme from the “requirements-pull” or “market-pull”, approach is “technology push.” Here we start with a solution (perhaps a new technology) and see what problems it might enable us to solve. The danger in this approach is to become enamored of “the solution” and neglect to ensure that it actually solves a problem. With technology push, it is likely that actual user requirements may be modified, or even

ignored in order to “force-fit” the desired solution. A historical example was the product known as Picture Phone introduced (and discontinued) in the 1960s when the advance of telecommunications technology first made possible the transmission and display of video as well as voice. Picture Phone, which allowed telephone users to see each other during a call, was a technological success but a market disaster. It turned out that callers generally don’t want to be seen, as a bit of unbiased market analysis would have disclosed.

Technology push should not be ignored, but if the goal is successful transition to the field with acceptable risk, the technology being pushed must be compared to alternative solutions against a real set of user requirements.

Aside from assuring that the “solution” actually solves the “problem,” requirements-driven design has a further advantage in that the requirements provide criteria against which a product’s successful development can be measured. Specifically, if the product was developed to address a set of quantified operational requirements, then its success is measured by Operational Test and Evaluation (OT&E) to validate that an end-user can use the product and achieve the stated operational goals.

Prior to OT&E, it is common practice to subject products to Developmental Test and Evaluation (DT&E). The purpose of DT&E is to verify that the product meets its technical specifications, which are the engineers’ interpretation of the operational requirements. Such DT&E does not obviate the need for OT&E, which validates that the engineers’ solution is not only technically successfully but also represents a successful interpretation of the end users’ needs, satisfying the original operational requirements (not just the technical specifications) when operated by representative users.

Often requirements are stated in terms of “threshold values” and “objective values,” where the “objective value” is the desired performance and the “threshold value” is the minimum acceptable performance. This formalism is useful in allowing stretch goals to be asserted without saddling the system development with unacceptable risk.

The Requirements Hierarchy and Traceability

To reiterate the definitions above, the documents that govern product realization include requirements, which define the problem, and specifications, which define the solution. Nevertheless, the hierarchy of requirements and specifications is more complex than that simple dichotomy, as previously discussed and revisited in Figure 8.

The Hierarchy is divided into two domains, operational requirements and technical requirements, highlighted in yellow and blue in the figure, representing the “problem space” and the “solution space” respectively. You will remember that the Capstone IPT process begins when S&T works with our customers to define and articulate capability gaps. The DHS stakeholder, representing the end users in the field (the operators), is also responsible for all operational requirements, from the top-level mission requirements to the detailed system-level operational requirements. It is important to articulate these

operational requirements in detail to avoid misunderstandings later in the product development life cycle. A system developer is responsible for translating the operational requirements into a system solution, documented in a hierarchy of technical specifications.

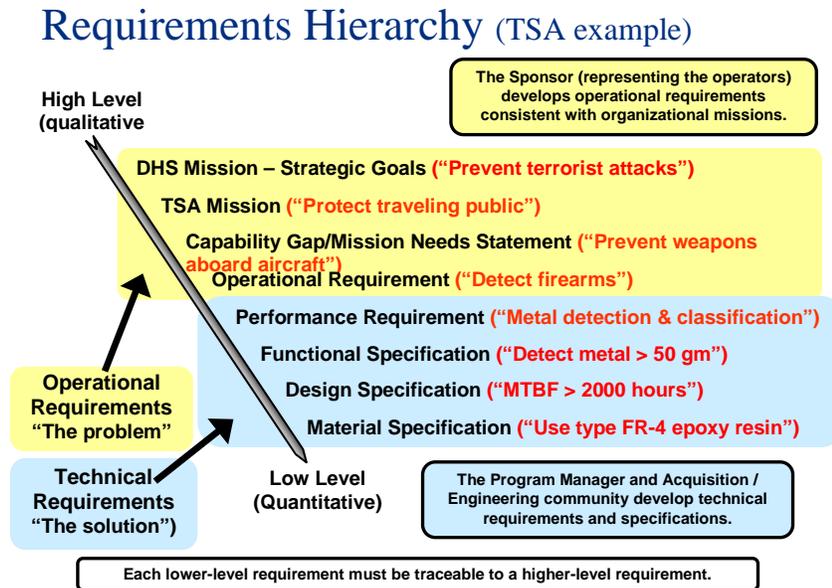


Figure 8. The Requirements Hierarchy drives the traceability of requirements from top to bottom.

The highest-level type of technical “specification” is actually called a performance “requirement.” A performance requirement actually represents a bridge from operational requirements to the engineering interpretation of those requirements. Put another way, in the course of developing a new system it is necessary to transform the system operational requirements, which are stated from a given Operating Component’s perspective as required outcomes of system action, into a set of system performance requirements, which are stated in terms of engineering characteristics.

Working through the requirements hierarchy, requirements development is the process of decomposing the problems broadly outlined in the capability gaps gleaned from the mission needs assessment.

The requirements and specifications are described below, first those that define the problem and then those that define the solution:

- **Problem Definition**

- **Mission Needs Statement (MNS)/Capability Gap** is required by the DHS Acquisition Review Process (Management Directive 102-01) and is developed by the DHS sponsor (S&T’s customer) who represents the end users and is the first step in the Capstone IPT process. The MNS provides a high-level description of the mission need (or, equivalently, capability gap), and is used to justify the initiation of an Acquisition program.

- **Operational Requirements Document (ORD)** is also required by the DHS Acquisition Review Process and, like the MNS, is developed by the DHS stakeholder. The ORD specifies operational requirements and a concept of operations (CONOPS), written from the point of view of the end user. The ORD is independent of any particular implementation, should not refer to any specific technologies and does not commit the developers to a design. A well written ORD states the problem that must be solved along with the necessary capabilities that a system must perform.
- **Solution Definition**
 - **Performance Requirements** represent a bridge between the operationally oriented view of the system defined in the ORD and an engineering-oriented view required to define the solution. Performance requirements are an interpretation, not a replacement of operational requirements. Performance requirements define the functions that the system and its subsystems must perform to achieve the operational objectives and define the performance parameters for each function. These definitions are in engineering rather than operational terms.
 - **Functional Specifications** define the system solution functionally, though not physically. Sometimes called the “system specification” or “A-Spec,” these specifications define functions at the system, subsystem, and component level including:
 - Configuration, organization, and interfaces between system elements
 - Performance characteristics and compatibility requirements
 - Human engineering
 - Security and safety
 - Reliability, maintainability and availability
 - Support requirements such as shipping, handling, storage, training and special facilities
 - **Design Specifications** convert the functional specifications of *what* the system is to do into a specification of *how* the required functions are to be implemented in hardware and software. The design specifications therefore govern the materialization of the system components.
 - **Material Specifications** are an example of lower-level supporting specifications that support the higher-level specifications. Material specifications define the required properties of materials and parts used to fabricate the system. Other supporting specifications include **Process Specifications** (defining required properties of fabrication processes such as soldering and welding) and **Product Specifications** (defining required properties of non-developmental items to be procured commercially).

Characteristics of Good Requirements

Requirements engineering is difficult and time-consuming, but must be done well if the final product or system is to be judged by the end users as successful. From the International Council of Systems Engineers (INCOSE) Requirements Working Group¹, here are eight attributes of good requirements:

- Necessary: Can the system meet prioritized, real needs without it? If yes, the requirement isn't necessary.
- Verifiable: Can one ensure that the requirement is met in the system? If not, the requirement should be removed or revised.
- Unambiguous: Can the requirement be interpreted in more than one way? If yes, the requirement should be clarified or removed. Ambiguous or poorly worded requirements can lead to serious misunderstandings and needless rework.
- Complete: Are all conditions under which the requirement applies stated? In addition, does the specification include all known requirements?
- Consistent: Can the requirement be met without conflicting with any other requirement? If not, the requirement should be revised or removed.
- Traceable: Is the origin (source) of the requirement known, and is there a clear path from the requirement back to its origin?
- Concise: Is the requirement stated simply and clearly?
- Standard constructs: Requirements are stated as imperative needs using "shall." Statements indicating "goals" or using the words "will" or "should" are not imperatives.

Developing Operational Requirements (ORDs): Customer Input

So far, we've discussed operational requirements but have not provided any insight into how to develop them. In an effort to provide a basic framework for the articulation and documentation of operational requirements, the operational requirements document (ORD) was created. ORDs provide a clear definition and articulation of a given problem, providing several layers of information that comprise the overall problem. Using resources such as this book and the accompanying template, we have tried to simplify and streamline the process of communicating requirements. ORDs can be used in Acquisition, Procurement, Internal Development, Commercialization and Outreach Programs – any situation that dictates detailed requirements (e.g. RFQ, BAA, RFP, RFI, etc.). It's clear to see that it's cost-effective and efficient for both DHS and all of its stakeholders to communicate needs clearly and effectively.

¹ Kar, Pradip and Bailey, Michelle. Characteristics of Good Requirements. International Council of Systems Engineers, Requirements Working Group. INCOSE Symposium, 1996. Found online: <http://www.afis.fr/nav/gt/ie/doc/Articles/CHARACTE.HTM>.

Let's first look at the contents of a typical Operational Requirements Document (ORD) shown in Figure 9.

OPERATIONAL REQUIREMENTS DOCUMENT

- 1.0 General Description of Operational Capability
 - 1.1. Capability Gap
 - 1.2. Overall Mission Area Description
 - 1.3. Description of the Proposed System
 - 1.4. Supporting Analysis
 - 1.5. Mission the Proposed System Will Accomplish
 - 1.6. Operational and Support Concept
 - 1.6.1. Concept of Operations
 - 1.6.2. Support Concept
- 2.0 Threat
- 3.0 Existing System Shortfalls
- 4.0 Capabilities Required
 - 4.1 Operational Performance Parameters
 - 4.2 Key Performance Parameters (KPPs)
 - 4.3 System Performance
 - 4.3.1 Mission Scenarios
 - 4.3.2 System Performance Parameters
 - 4.3.3 Interoperability
 - 4.3.4 Human Interface Requirements
 - 4.3.5 Logistics and Readiness
 - 4.3.6 Other System Characteristics
- 5.0 System Support
 - 5.1 Maintenance
 - 5.2 Supply
 - 5.3 Support Equipment
 - 5.4 Training
 - 5.5 Transportation and Facilities
- 6.0 Force Structure
- 7.0 Schedule
- 8.0 System Affordability

Figure 9. The Contents of an Operational Requirements Document

The complexity of the intended system and its operational context will govern the required level of detail in the ORD. The most difficult sections to develop are typically Section 4.0, which describes the capabilities required of the system to be developed, and Section 1.6, which describes the operational and support concepts.

There is no “silver bullet” to solve the potential challenges in developing an ORD, but since the issues are universal, there is a wealth of literature that offers approaches to requirements development. As an example, here are nine requirements-elicitation techniques described in the *Business Analyst Body of Knowledge* (from the International Institute of Business Analysis)².

² International Institute of Business Analysis. *A Guide to the Business Analyst Body of Knowledge*, Release 1.6. 2006. Found online: http://www.theiiba.org/Content/NavigationMenu/Learning/BodyofKnowledge/Version16/BOKV1_6.pdf.

1. Brainstorming

- Purpose
 - An excellent way of eliciting many creative ideas for an area of interest. Structured brainstorming produces numerous creative ideas.
- Strengths
 - Able to elicit many ideas in a short time period.
 - Non-judgmental environment enables outside-the-box thinking.
- Weaknesses
 - Dependent on participants' creativity.

2. Document Analysis

- Purpose
 - Used if the objective is to gather details of the “As Is” environment such as existing standard procedures or attributes that need to be included in a new system.
- Strengths
 - Not starting from a blank page.
 - Leveraging existing materials to discover and/or confirm requirements.
 - A means to crosscheck requirements from other elicitation techniques such as interviews, job shadowing, surveys or focus groups.
- Weaknesses
 - Limited to “as-is” perspective.
 - Existing documentation may not be up-to-date or valid.
 - Can be a time-consuming and even tedious process to locate the relevant information.

3. Focus Group

- Purpose
 - A means to elicit ideas and attitudes about a specific product, service or opportunity in an interactive group environment. The participants share their impressions, preferences and needs, guided by a moderator.
- Strengths
 - Ability to elicit data from a group of people in a single session saves time and costs as compared to conducting individual interviews with the same number of people.
 - Effective for learning people's attitudes, experiences and desires.
 - Active discussion and the ability to ask others questions creates an environment where participants can consider their personal view in relation to other perspectives.
- Weaknesses
 - In the group setting, participants may be concerned about issues of trust, or may be unwilling to discuss sensitive or personal topics.

- Data collected (what people say) may not be consistent with how people actually behave.
- If the group is too homogenous, the group's responses may not represent the complete set of requirements.
- A skilled moderator is needed to manage the group interactions and discussions.
- It may be difficult to schedule the group for the same date and time.

4. Interface Analysis

- Purpose
 - An interface is a connection between two components. Most systems require one or more interfaces with external parties, systems or devices. Interface analysis is initiated by project managers and analysts to reach agreement with the stakeholders on what interfaces are needed. Subsequent analysis uncovers the detailed requirements for each interface.
- Strengths
 - The elicitation of the interfaces' functional requirements early in the system life cycle provides valuable details for project management:
 - Impact on delivery date. Knowing what interfaces are needed, their complexity and testing needs enables more accurate project planning and potential savings in time and cost.
 - Collaboration with other systems or projects. If the interface to an existing system, product or device and the interface already exist, it may not be easily changed. If the interface is new, then the ownership, development and testing of the interface needs to be addressed and coordinated in both projects' plan. In either case, eliciting the interface requirements will require negotiation and cooperation between the owning systems.
- Weaknesses
 - Does not provide an understanding of the total system or operational concept since this technique only exposes the inputs, outputs and key data elements related to the interfaces.

5. Interview

- Purpose
 - A systematic approach to elicit information from a person or group of people in an informal or formal setting by asking relevant questions and documenting the responses.
- Strengths
 - Encourages participation and establishes rapport with the stakeholder.
 - Simple, direct technique that can be used in varying situations.
 - Allows the interviewer and participant to have full discussions and explanations of the questions and answers.
 - Enables observations of non-verbal behavior.

- The interviewer can ask follow-up and probing questions to confirm own understanding.
- Maintain focus using clear objectives for the interview that are agreed upon by all participants and can be met in the time allotted.
- Weaknesses
 - Interviews are not an ideal means of reaching consensus across a group of stakeholders.
 - Requires considerable commitment and involvement of the participants.
 - Training is required to conduct good interviews. Unstructured interviews, especially, require special skills. Facilitation/virtual facilitation and active listening are a few of them.
 - Depth of follow-on questions may be dependent on the interviewer's knowledge of the operational domain.
 - Transcription and analysis of interview data can be complex and expensive.
 - Resulting documentation is subject to interviewer's interpretation.

6. Observation

- Purpose
 - A means to elicit requirements by assessing the operational environment. This technique is appropriate when documenting details about current operations or if the project intends to enhance or change a current operational concept.
- Strengths
 - Provides a realistic and practical insight into field operations by getting a hands-on feel for current operations.
 - Elicits details of informal communication and ways people actually work around the system that may not be documented anywhere.
- Weaknesses
 - Only possible for existing operations.
 - Could be time-consuming.
 - May be disruptive to the person being shadowed.
 - Unusual exceptions and critical situations that happen infrequently may not occur during the observation.
 - May not well work if current operations involve a lot of intellectual work or other work that is not easily observable.

7. Prototyping

- Purpose
 - Prototyping, when used as an elicitation technique, aims to uncover and visualize user requirements before the system is designed or developed.

- Strengths
 - Supports users who are more comfortable and effective at articulating their needs by using pictures or hands-on prototypes, as prototyping lets them “see” the future system’s interface.
 - A prototype allows for early user interaction and feedback.
 - A throwaway prototype is an inexpensive means to quickly uncover and confirm user interface requirements.
 - A revolutionary prototype can demonstrate what is feasible with existing technology, and where there may be technical gaps.
 - An evolutionary prototype provides a vehicle for designers and developers to learn about the users’ interface needs and to evolve system requirements.
- Weaknesses
 - Depending on the complexity of the target system, using prototyping to elicit requirements can take considerable time if the process is bogged down by the “how’s” rather than “what’s”.
 - Assumptions about the underlying technology may need to be made in order to present a starting prototype.
 - A prototype may lead users to set unrealistic expectations of the delivered system’s performance, reliability and usability characteristics.

8. Requirements Workshop

- Purpose
 - A requirements workshop is a structured way to capture requirements. A workshop may be used to scope, discover, define, prioritize and reach closure on requirements for the target system. Well-run workshops are considered one of the most effective ways to deliver high quality requirements quickly. They promote trust, mutual understanding, and strong communications among the project stakeholders and project team, produce deliverables that structure, and guide future analysis.
- Strengths
 - A workshop can be a means to elicit detailed requirements in a relatively short period of time.
 - A workshop provides a means for stakeholders to collaborate, make decisions and gain a mutual understanding of the requirements.
 - Workshop costs are often lower than the cost of performing multiple interviews.
 - A requirements workshop enables the participants to work together to reach consensus which is typically a cheaper and faster approach than doing serial interviews as interviews may yield conflicting requirements and the effort needed to resolve those conflicts across all interviewees can be very costly.
 - Feedback is immediate, if the facilitator’s interpretation of requirements is fed back immediately to the stakeholders and confirmed.

- Weaknesses
 - Due to stakeholders availability it may be difficult to schedule the workshop.
 - The success of the workshop is highly dependent on the expertise of the facilitator and knowledge of the participants.
 - Requirements workshops that involve too many participants can slow down the workshop process thus negatively affecting the schedule. Conversely, collecting input from too few participants can lead to overlooking requirements that are important to users, or to specifying requirements that do not represent the needs of the majority of the users.

9. Survey/Questionnaire

- Purpose
 - A means of eliciting information from many people, anonymously, in a relatively short time. A survey can collect information about customers, products, operational practices and attitudes. A survey is often referred to as a questionnaire.
- Strengths
 - When using ‘closed-ended’ questions, effective in obtaining quantitative data for use in statistical analysis.
 - When using open-ended questions, the survey results may yield insights and opinions not easily obtainable through other elicitation techniques.
 - Does not typically require significant time from the responders.
 - Effective and efficient when stakeholders are not located at one place.
 - May result in large number of responses.
 - Quick and relatively inexpensive to administer.
- Weaknesses
 - Use of open-ended questions requires more analysis.
 - To achieve unbiased-results, specialized skills in statistical sampling methods are needed when the decision has been made to survey a sample subset.
 - Some questions may be left unanswered or answered incorrectly due to their ambiguous nature.
 - May require follow up questions or more survey iterations depending on the answers provided.
 - Not well suited for collecting information on actual behaviors.

Addressing Requirements versus Proposing Solutions

When employing efforts to elicit and explain requirements using any of these methods, it is imperative to steadfastly avoid requirements that define potential solutions or otherwise restrict the potential solution space. Again, requirements only deal with the problem at hand and do not discuss the preferred or desired tool or way to go about solving the problem. Any standards or limitations that a system must address within a

given scenario are important to mention within an ORD, but entire solution sets may not be discounted as potential scientific advances may make certain technologies feasible. While it is necessary and useful to understand the current state-of-the-art within a given technology space and knowledge about potential solutions that may already be in development, requirements are meant to simply define problems. Properly drafted requirements allow for a variety of solutions, each with their own advantages and disadvantages, for consideration as potential ways to address a problem. Solution-agnostic requirements prevent limiting and defining the outcome of product realization. Within the context of the Operational Requirements Document Template described in detail below, the solution definition aspect of the Requirements Hierarchy is purposefully not addressed. This is useful given that an open and honest review of one's needs might show that a preconceived notion about a desired solution may turn out not to be the best solution, or that modifications to existing products or services may be necessary and useful to end users.

The following insert provides the Operational Requirements Document template. This template guides you through drafting a new ORD by describing the information that should be captured in each section of the document. This template is useful in organizing and delineating the problem to be solved. Several important topics are covered by the template and it assists in presenting many questions that must be addressed in order to articulate fully and clearly the desired outcome from deploying a system to address a problem.

Operational Requirements Document Template

1. General Description of Operational Capability

In this section, summarize the capability gap which the product or system is intended to address, describe the overall mission area, describe the proposed system solution, and provide a summary of any supporting analyses. Additionally, briefly describe the operational and support concepts.

1.1. Capability Gap

Describe the analysis and rationale for acquiring a new product or system, and identify the DHS Component, which contains or represents the end users. Also, name the Capstone IPT, if any, which identified the capability gap.

1.2. Overall Mission Area Description

Define and describe the overall mission area to which the capability gap pertains, including its users and its scope

1.3. Description of the Proposed System

Describe the proposed product or system. Describe how the product or system will provide the capabilities and functional improvements needed to address the capability gap. Do not describe a specific technology or system solution. Instead, describe a conceptual solution for illustrative purposes.

1.4. Supporting Analysis

Describe the analysis that supports the proposed system. If a formal study was performed, identify the study and briefly provide a summary of results.

1.5. Mission the Proposed System Will Accomplish

Define the missions that the proposed system will be tasked to accomplish.

1.6. Operational and Support Concept

1.6.1. Concept of Operations

Briefly describe the concept of operations for the system. How will the system be used, and what is its organizational setting? It is appropriate to include a graphic that depicts the system and its operation. Also, describe the system's interoperability requirements with other systems.

1.6.2. Support Concept

Briefly describe the support concept for the system. How will the system (hardware and software) be maintained? Who will maintain it? How, where, and by whom will spare parts be provisioned? How, where, and by whom will operators be trained?

2. Threat

If the system is intended as a countermeasure to a threat, summarize the threat to be countered and the projected threat environment.

3. Existing System Shortfalls

Describe why existing systems cannot meet current or projected requirements. Describe what new capabilities are needed to address the gap between current capabilities and required capabilities.

4. Capabilities Required

4.1. Operational Performance Parameters

Identify operational performance parameters (capabilities and characteristics) required for the proposed system. Articulate the requirements in output-oriented and measurable terms. Use Threshold/Objective format and provide criteria and rationale for each requirement.

4.2. Key Performance Parameters (KPPs)

The KPPs are those attributes or characteristics of a system that are considered critical or essential. Failure to meet a KPP threshold value could be the basis to reject a system solution.

4.3 System Performance.

4.3.1 Mission Scenarios

Describe mission scenarios in terms of mission profiles, employment tactics, and environmental conditions.

4.3.2 System Performance Parameters

Identify system performance parameters. Identify KPPs by placing an asterisk in front of the parameter description.

4.3.3 Interoperability

Identify all requirements for the system to provide data, information, materiel, and services to and accept the same from other systems, and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together.

4.3.4 Human Interface Requirements

Discuss broad cognitive, physical, and sensory requirements for the operators, maintainers, or support personnel that contribute to, or constrain, total system performance. Provide broad staffing constraints for operators, maintainers, and support personnel.

4.3.5 Logistics and Readiness

Describe the requirements for the system to be supportable and available for operations. Provide performance parameters for availability, reliability, system maintainability, and software maintainability.

4.3.6 Other System Characteristics

Characteristics that tend to be design, cost, and risk drivers.

5. System Support

Establish support objectives for initial and full operational capability. Discuss interfacing systems, transportation and facilities, and standardization and interoperability. Describe the support approach including configuration management, repair, scheduled maintenance, support operations, software support, and user support (such as training and help desk).

5.1 Maintenance

Identify the types of maintenance to be performed and who will perform the maintenance. Describe methods for upgrades and technology insertions. Also, address post-development software support requirements.

5.2 Supply

Describe the approach to supplying field operators and maintenance technicians with necessary tools, spares, diagnostic equipment, and manuals.

5.3 Support Equipment

Define the standard support equipment to be used by the system. Discuss any need for special test equipment or software development environment

5.4 Training

Describe how the training will ensure that users are certified as capable of operating and using the proposed system.

5.5 Transportation and Facilities

Describe how the system will be transported to the field, identifying any lift constraints. Identify facilities needed for staging and training.

6. Force Structure

Estimate the number of systems or subsystems needed, including spares and training units. Identify organizations and units that will employ the systems being developed and procured, estimating the number of users in each organization or unit.

7. Schedule

To the degree that schedule is a requirement, define target dates for system availability. If a distinction is made between Initial Capability and Full Operational Capability,

clarify the difference between the two in terms of system capability and/or numbers of fielded systems.

8. System Affordability

Identify a threshold/objective target price to the user at full-rate production. If price is a KPP, include it in the section on KPPs above.

*Please Note: See Appendix B for a full set of real-world examples ORDs that clearly illustrate how to effectively use this template and other previously described requirements elicitation methods.

DHS Markets Create Opportunities for the Private Sector

Simply put, the mission of the Department of Homeland Security (DHS) is to protect our nation's most valuable asset -- our people. It is nowhere more important than to provide these groups with the necessary resources and capabilities that enable them to ensure mission success. Addressing the needs and requirements of DHS' myriad stakeholders continues to be a challenge requiring new ideas to gather resources and innovative technologies and products effective at combating the numerous threats facing our nation.

DHS experienced several challenges merging twenty-two disparate organizations, along with taking responsibility for the millions of our nation's first responders and CIKR owners and operators, into a cohesive organization with a unified mission and culture. Those familiar with Merger and Acquisition (M&A) activities realize that while integration of organizations poses difficulties, it also represents opportunities to infuse new processes and values into the newly created organization. Through both "top-down" and "bottom-up" approaches, DHS has been successful in developing, socializing and now implementing an innovative commercialization framework that has started to gain traction throughout the agency. The creation of a "Commercialization Mindset" has caught the attention of DHS managers and employees and has been embraced by senior management because of its significant benefits to the Department's internal and external activities.

Many situations arise within the Department, First Responder Community and Private sector where there is a need for widely distributed products. Recognizing this fact, the Department recently began fostering a "Commercialization Mindset"³ in order to leverage the vast capability and resources of the private sector through innovative "win-win" public-private partnerships stressing the need for detailed requirements. Commercialization represents another "tool in the toolbox" that can be used to provide much needed products and services to the DHS stakeholders. While the development of highly specialized products using traditional Acquisition channels is still relevant to the Department, the fact that DHS is a conduit to large markets is highly advantageous for its stakeholders. The process of partnering with the private sector solution providers to work cooperatively on many of the steps in the system engineering life cycle will allow more groups to be involved in developing competing solutions to DHS' customer needs, when low-unit-volume custom systems are not required. Not only is this a new way of thinking about developing and procuring products, it necessitates clear and precise communications between the public and private sectors.

³ See, for example, *Developing Operational Requirements, Version 2, Product Realization Chart, DHS Implements a Commercialization Process* and other valuable resources online at http://www.dhs.gov/xres/programs/gc_1211996620526.shtm

In order for solution providers to invest their valuable time, money and resources to develop products and services for use by DHS operating components, first responder communities, CIKR owners and operators and other stakeholders, the DHS commercialization process relies on providing them with two key pieces of information:

- 1) A clear and detailed delineation and explanation of the operational requirements, and
- 2) A conservative estimate of the potential available market for a potential commercialization partner to offer potential solution(s).

Resources like this guide are useful aides in addressing the first piece of developing cooperative partnerships.

Commercialization Office Initiatives at DHS

As a natural extension of the Capstone IPT process, the Department's Commercialization Office has taken the lead in developing innovative programs and processes that actively seek to foster public-private partnerships to develop and deploy much needed capabilities with the speed-of-execution and efficiency needed to match the demands of DHS' stakeholders. The Commercialization Office focuses on bringing improved clarity and communication of stakeholders' needs across the Department and to private sector partners who have resources to assist in product and technology development. Working in a constructive way in which all the participants, including the private sector, public sector, and taxpayer, benefit enables the high probability of expediting the cost effective and efficient development of products and services to meet the unsatisfied needs and wants of the Department, its operating components, first responders and the CIKR owners and operators.

The Commercialization Office, found within S&T's Office of Transition, is responsible for accelerating the delivery of enhanced technological capabilities to meet the requirements and close the capability gaps to support DHS agencies and its stakeholders in accomplishing their missions. The major activities that enable the accomplishment of the goals of the Commercialization Office are the requirements development initiative, commercialization process, creation of public-private partnerships and outreach to the private sector.

To facilitate the development of new products and technologies a clear understanding is necessary so that efforts are well coordinated and move with a common purpose. To build upon the capability gaps that are outputs of the Capstone IPT process, DHS recognized the importance in developing operational requirements at an early stage in product development. As previously stated, this discipline enables DHS personnel to articulate, in detail, a given problem and its associated requirements. Stakeholders can communicate those needs to both internal and external audiences. This effort addresses a long-standing need for DHS to fully articulate its requirements and explain in detail the capabilities necessary for mission success. Once again, the requirements hierarchy shows how an Operational Requirement Document (ORD) takes a capability gap to "much higher resolution," a necessary step required for product developers to assist DHS in its

goal of expediting the deployment of cost-effective and efficient widely distributed products.

Through the publication of a number of books including the *Requirements Development Guide* and *Developing Operational Requirements*⁴, the Commercialization Office provides resources for understanding the importance of requirements and guidelines and templates for creating ORDs. The clear communication of requirements ensures that all parties involved are “on the same page” and that product and technology development moves along clearly defined paths.

Market Potential is Catalyst for Rapid New Product Development

It is important to understand not only the detailed operational requirements necessary to provide DHS stakeholders with mission-critical capabilities, but also understand the volume of potential users of these solutions. DHS itself can represent a substantial potential available market; in many instances requiring hundreds, if not thousands of product or service units to address unsatisfied needs. Couple to this the fact that DHS is responsible for so many ancillary markets (e.g. first responders, critical infrastructure and key resource owners and operators, etc.) representing large potential available markets, it is evident that substantial business opportunities exist for the private sector as these large pools of potential customers and users represent the “lifeblood” for businesses (See Figure 10).

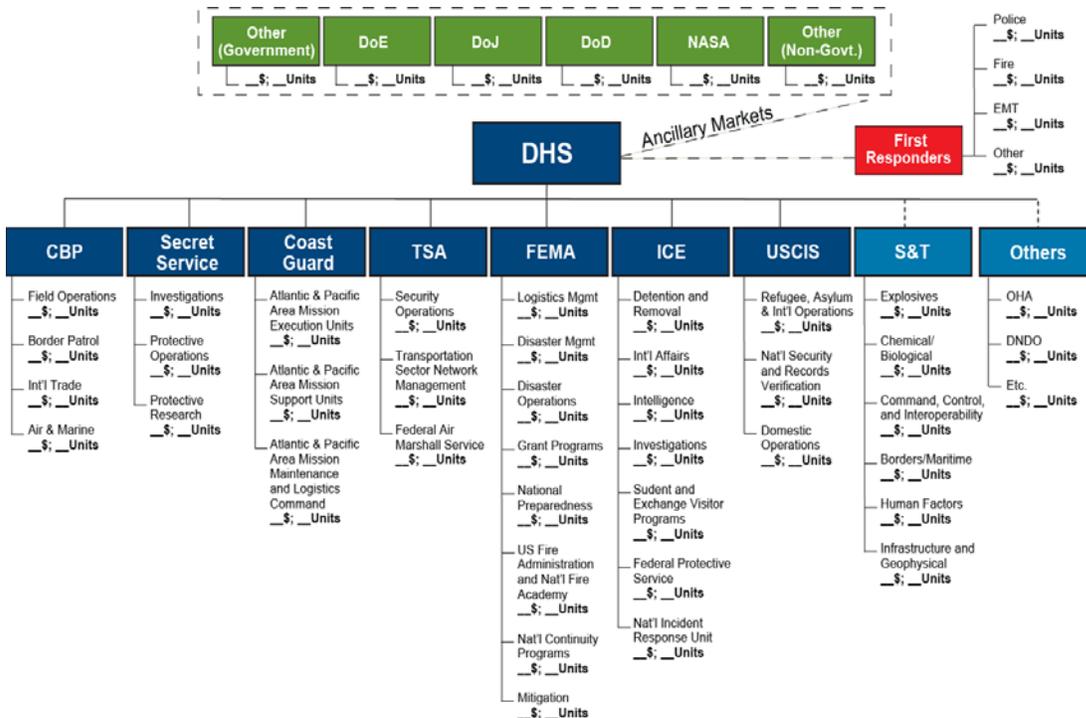


Figure 10. While the development of highly specialized products using traditional Acquisition channels is still relevant to the Department, the fact that DHS is a conduit to such large markets is highly advantageous for its stakeholders.

In order to provide opportunities for a greater number of private sector entities to get involved in addressing the needs of these markets, it is the hope that the market analysis and proper articulation of requirements encourages innovative thinking on the part of the private sector to market valuable solutions given that many needs may be shared across both public and private sector communities.

Keep it Simple Make it Easy

The DHS commercialization process is based upon the simple premise that the private sector is willing and able to use its own money, resources, expertise and experience to develop and produce fully developed products and services for DHS if significant market potential exists. The private sector has shown remarkable interest in devoting its time and resources to such activities, if and when an attractive business case can be made related to large revenue/profit opportunities. Market analyses clearly demonstrate that large potential available markets exist for DHS and its ancillary markets. In order to actively engage with the private sector DHS must share two pieces of critical information: 1. detailed operational requirement(s), and 2. a conservative estimate of the potential available market(s). This information can then be used to generate a business case for possible private sector participation in the program.

In its new Commercialization model, S&T acts as a facilitator between its customers - DHS' operating components and ancillary markets - and the private sector entities who may potentially develop products for use by DHS' stakeholders. S&T must work with its valued customers in the creation of ORDs that accurately reflect their mission-critical operational requirements through active participation in the requirements development initiatives. S&T also conducts market surveys and technology scans to ensure that needed technical capabilities and/or products can be made accessible in response to the requirements of generated ORDs. This analysis also leads to understandings of the number of potential users and applications for potential solutions. This allows the private sector to understand in a clear and transparent way what the Department and its customers need in order to use their time, money, and resources to create products, services or technologies where market potential is large. Oftentimes, private sector entities have products in development that are closely aligned with current homeland security capability gaps and can be transitioned to the field rapidly and cost-effectively.

SECURE™ and FutureTECH™

The Commercialization Office created two innovative public-private partnership programs to engage the private sector for cooperative product development efforts. The SECURE™ (System Efficacy through Commercialization Utilization Relevance and Evaluation) program seeks to find highly developed (TRL 5-9) private sector product offerings aligned to DHS generated and vetted ORDs posted on the DHS website. Its sister program, FutureTECH™, focuses on the long-term needs of the Department that require the development of new technologies (TRL 1-6) to address future capability gaps. We have demonstrated through the SECURE™ and FutureTECH™ programs that the

federal government can engage and influence - in a positive way - the private sector by offering detailed requirements and conservative estimates of market potential. The reason that these partnerships are successful is simple and straightforward. Firms spend significant resources in trying to understand market needs and potential through their business and market development efforts. By offering this information, government saves the private sector both time and money while demonstrating its genuine desire to work cooperatively to develop technologies and products to meet DHS stakeholders' needs in a cost-effective and efficient way that benefits the private and public sectors – but also, most importantly, to the American taxpayers' benefit.

Through the SECURE Program, the Department provides to potential solution providers detailed operational requirements and a conservative estimate of the potential available market(s) offered by DHS stakeholders. In exchange for this valuable information, the private sector offers deployable products and services (along with recognized third party test and evaluation data) that meet these stated requirements in an open and free way that creates an ergonomic “clearinghouse of solutions” available to DHS stakeholders. Because of the success and “win-win-win” nature of this program in that it provides benefits for the American taxpayer, the private sector and DHS, DHS-S&T recently introduced the FutureTECH™ Program that describes the long-term capabilities/technologies required by DHS stakeholders.

FutureTECH™ identifies and focuses on the future needs of the Department as fully deployable technologies and capabilities, in some cases, are not readily available in the private sector or Federal government space. While the SECURE™ Program is valuable to all DHS operating components, organizational elements and DHS stakeholders, FutureTECH™ is intended for DHS S&T use only, particularly in the fields/portfolios related to Research and Innovation.

After providing independent third-party testing and evaluation of potential products, services, or technologies to show they do in fact meet or exceed the specifications listed in the detailed operational requirements, private sector entities can potentially enter into a partnership with the Department in order to deliver commercial-off-the-shelf products to the Department's stakeholders. In addition to providing products to DHS and its stakeholders, these partnership programs, SECURE™⁵ and FutureTECH™⁶, give the much needed assurance to the First Responder and CIKR communities that a certified product or service works as specified and is aligned to the requirements document.

Outreach to the Private Sector

In order for these programs to be successful in providing needed products, services, and technologies to DHS and its stakeholders, partnerships with the private sector are imperative. The private sector outreach efforts of the Commercialization Office are

⁵ Cellucci, Thomas A. “Commercialization Office: Offering Transformational Change Beyond DHS,” June 2009.

⁶ Cellucci, Thomas A. “FutureTECH: Guidance to Understanding Future DHS S&T Critical Research/Innovation Focus Areas,” April 2009.

designed to provide information to the public on “How to do Business with DHS.” Efforts demonstrate the value of engaging in mutually beneficial relationships to provide business opportunities to produce products/services to DHS components and ancillary markets. The private sector outreach efforts of the Commercialization Office center on notifying the private sector about opportunities that exist for partnership and business development to address the needs of the Department.

Through websites⁷, speeches, conferences, seminars, and publications the Commercialization Office is able to provide to the private sector information on partnership opportunities and helpful resources and contacts to foster a public-private partnership. A “full response package” can be requested that includes more background on the SECURE™ and FutureTECH™ programs as well as a template company overview that can be submitted and entered into our repository that is available for the whole Department to review.

Doing business with DHS creates a number of ancillary benefits for the private sector. The communication of detailed requirements and conservative estimates of potential available markets helps guide businesses as they continue to pursue new opportunities. The involvement of the Venture Capital and Angel Investor communities is a critical function in assisting small businesses and start-up companies with innovative new technologies for the homeland security market place. These groups are traditionally entrepreneurial seeking opportunities to advance cutting-edge technology with a primary focus on speed-of-execution. Partnerships within the private sector itself are fostered regularly to bring fully deployable solutions to these new markets. Companies are enabled to approach potential partnerships with a stronger business case based on a credible understanding of the needs of their potential customers that show true business opportunities. Funding new and innovative technologies that have the potential to address numerous large markets is an attractive opportunity for venture capitalists and angel investors. In addition, there has been a marked increase in the number of strategic partnerships between small businesses and large companies as each has something to offer.

Small businesses are the “engines of innovation”⁸. These small businesses are creative entities, offering new solutions and ideas to solve many complex challenges. However, many small businesses lack the resources for proper business development and sales development practices. In these cases strategic partnerships offer opportunities to grow sales and market channels that can bring their innovative technologies to the field where they can be of the greatest benefit. Figure 4 below is a benefit analysis demonstrating how all participants receive positive outcomes as a result of fostering public-private partnerships.

⁷ See Commercialization Office websites at www.DHS.gov. Homepage found at: http://www.dhs.gov/xabout/structure/gc_1234194479267.shtm.

⁸ Cellucci, Thomas A. “Focus on Small Business: Opportunities Abound for the Engines of Innovation,” March 2009.

Benefit Analysis – “Win-Win-Win”		
Taxpayers	Public Sector	Private Sector
1. Citizens are better protected by DHS personnel using mission critical products	1. Improved understanding and communication of needs	1. Save significant time and money on market and business development activities
2. Tax savings realized through Private Sector investment in DHS	2. Cost-effective and rapid product development process saves resources	2. Firms can genuinely contribute to the security of the Nation
3. Positive economic growth for American economy through creation of jobs and business opportunities	3. Monies can be allocated to perform greater number of essential tasks	3. Successful products share in the “imprimatur of DHS”; providing assurance that products really work.
4. Possible product “spin-offs” can aid other commercial markets	4. End users receive products aligned to specific needs	4. Significant business opportunities with sizeable DHS and ancillary markets
5. Customers ultimately benefit from COTS produced within the Free Market System – more cost effective and efficient product development	5. End users can make informed purchasing decisions with tight budgets	5. Potential strategic partnership and commercialization opportunities between small, medium and large businesses result

Figure 11 The Commercialization Office’s public-private partnerships are viewed positively by DHS stakeholders. The success of the program lies in the fact that all participants receive significant benefits.

For many private sector solution providers the potential to do business with DHS has never been greater. New programs have opened significant business opportunities to work in cooperative public-private partnerships. The private sector can now play a critical role in developing needed capabilities for DHS’ stakeholders in a freely competitive way that shows demonstrable benefits for many different groups. New collaborative business practices will enable DHS to field fully developed products with a speed-of-execution not seen before in many government programs. Continued participation and engagement through these partnership programs will only increase as more requirements are gathered and shared creating the opportunities necessary for businesses to get involved. The private sector shows everyday its willingness to be an active partner through genuine interest in ensuring that DHS’ stakeholders are better able to carry out their mission and protect the people of the United States. DHS will continue to enable these relationships with the goal of facing the many challenges that lay ahead.

Summary

This document has offered a brief summary of the Capstone IPT process, the need for communication between the CIKR communities and S&T, the role of requirements at DHS. Particular emphasis has been given to the requirements hierarchy, including defining capability gaps and demonstrating that operational requirements govern the development of an end-user system. Acknowledging the difficulty of requirements development, it presented nine best practices to elicit requirements from an end-user community and eight criteria to judge the quality of requirements. It illustrated how an ORD is generated using an ORD template. We also provide several real-world examples of ORDs to assist in drafting new ORDs for new problems and needs. The additional readings listed below are a collection of short articles that provide a number of explanations on the importance of requirements development as well as some additional methods not described in this resource. We encourage you to seek out supplemental information on the topic of requirements development as this book is just one resource among many that can be of value to those developing and understanding requirements in a detailed and thoughtful way. Please take the effort to review the carefully prepared appendixes that follow, as they reveal important and practical knowledge in developing operational requirements to enhance our nation's security in a cost-effective and efficient manner.

Additional Requirements Development Readings

AntFarm, Inc. "Uncovering Hidden Customer Needs to Grow Your Services Business". 2007. http://www.antfarm-inc.com/docs/Growing_Services.pdf.

Byrd, T.A., Cossick, K.L. and Zmud, R.W. A Synthesis of Research of Requirements Analysis and knowledge Acquisition Techniques. MIS Quarterly, 16 (1). 117-138.

Cellucci, Thomas A. "DHS: Leading the Way to Help the Private Sector Help Itself." February 2009. http://www.dhs.gov/xlibrary/assets/st_critical_infrastructure_key_resources_article.pdf.

Cellucci, Thomas A. "Harnessing the Valuable Experience and Resources of the Private Sector for the Public Good: DHS' Entry into Commercialization." February 2009. http://www.dhs.gov/xlibrary/assets/st_harnessing_the_value_of_the_private_sector2.pdf.

Cellucci, Thomas A. "Developing Operational Requirements, Version 2.0." November 2008. http://www.dhs.gov/xlibrary/assets/Developing_Operational_Requirements_Guides.pdf.

- Cellucci, Thomas A. "Developing Operational Requirements." May 2008.
- Cellucci, Thomas A. "Requirements Development Guide." April 2008.
- Coplenish Consulting Group. "New Product Best Practices: Over 100 Ideas for Better NPD". 2004. <http://www.coplenish.com/FreeStuffPages/npdbp.pdf>.
- David. "Undreamt Requirements." Weblog entry. David's Software Development Survival Guide. March 12, 2007. <http://softwaresurvival.blogspot.com/2007/03/undreamt-requirements.html>.
- Davis, Alan. "Just Enough Requirements Management, Part I." CodeGear. November 10, 2004. <http://conferences.codegear.com/print/32301>.
- Derby, Esther. Building a Requirements Foundation Through Customer Interviews. Amplifying Your Effectiveness. 2004. <http://www.ayeconference.com/buildingreqtsfoundation/>.
- Graham, Ian. Requirements Engineering and Rapid Development: An Object Oriented Approach. Addison-Wesley Professional. 1999.
- Japenga, Robert. "How to Write a Software Requirements Specification." Micro Tools, Inc. 2003. <http://www.microtoolsinc.com/Howsrs.php>.
- Korman, Jonathan. "Putting People Together to Create New Products." Cooper. 2001. http://www.cooper.com/insights/journal_of_design/articles/putting_people_together_to_cre.html.
- Kotonya, G. and Sommerville, I. Requirements Engineering: Processes and Techniques. John Wiley & Sons, 1998.
- Larson, Elizabeth, and Richard Larson. "Projects without Borders: Gathering Requirements on a Multi-Cultural Project." The Project Manager Homepage. August 3, 2006. <http://www.allpm.com/print.php?sid=1587>.
- Miller, Hal. "Customer Requirements Specifications." The Usenix Magazine. Vol. 30, No. 2. 2004. <http://www.usenix.org/publications/login/2005-04/pdfs/miller0504.pdf>.
- Olshavsky, Ryan. "Bridging the Gap with Requirements Definition." Cooper. 2002. http://www.cooper.com/insights/journal_of_design/articles/bridging_the_gap_with_requirements_1.html .
- Pande, Peter S., Robert Neuman, and Roland Cavanagh. "Defining Customer Requirements: Six Sigma Roadmap Step 2." *The Six Sigma Way: How GE, Motorola,*

and Other Top Companies are Honing Their Performance. McGraw-Hill, New York. 2000

<http://www.sixsig.info/research/chapter13.php>.

"Requirements analysis." *Wikipedia, The Free Encyclopedia*. Wikimedia Foundation, Inc. April 8, 2008.

http://en.wikipedia.org/w/index.php?title=Requirements_analysis&oldid=204196812.

Sehlhorst, Scott. "Elicitation Techniques for Processes, Rules, and Requirements." Weblog entry. Tyner Blain. September 13, 2007.

<http://tynerblain.com/blog/2007/09/13/elicitation-techniques-2/>.

Sehlhorst, Scott. "Ten Requirements Gathering Techniques." Weblog entry. Tyner Blain. November 21, 2006.

<http://tynerblain.com/blog/2006/11/21/ten-requirements-gathering-techniques/>.

Silverman, Lori L., "Customers or Consumers? Focus or Obsession?" Partners for Progress. 2000.

<http://www.partnersforprogress.com/Articles/Customers%20or%20Consumers.pdf>.

Sisson, Derek. "Requirements and Specifications". Philosophe.com. January 9, 2000.

<http://www.philosophe.com/design/requirements.html>.

U.S. Department of Defense. Defense Acquisition Guidebook, Chapter 4. Dec. 2004.

https://akss.dau.mil/DAG/TOC_GuideBook.asp?sNode=R&Exp=Y.

Ward, James. "It Is Still the Requirements: Getting Software Requirements Right."

Sticky Minds. June 7, 2005. http://www.stickyminds.com/s.asp?F=S9150_ART_2.

Wieggers, Karl E., and Sandra McKinsey. "Accelerate Development by Getting Requirements Right." 2007.

<http://www.serena.com/docs/repository/products/dimensions/accelerate-developme.pdf>.

Wilson, William. "Writing Effective Requirements Specifications." NASA Software Assurance Technology Center. April 1997.

http://satc.gsfc.nasa.gov/support/STC_APR97/write/writert.html.

Winant, Becky. "Requirement #1: Ask Honest Questions." Sticky Minds. April 3, 2002.

http://www.stickyminds.com/s.asp?F=S3264_COL_2.

Zeller, Randel L. and Thomas A. Cellucci. "First Responder Capstone IPT: Delivering Solutions to First Responders." May 2009.

http://www.dhs.gov/xlibrary/assets/st_comm_first_responder_capstone_ipt_book.pdf

Appendix A:

National Infrastructure Protection Plan



National Infrastructure Protection Plan

Partnering to enhance protection and resiliency

2009



Preface



Michael Chertoff

Risk in the 21st century results from a complex mix of manmade and naturally occurring threats and hazards, including terrorist attacks, accidents, natural disasters, and other emergencies. Within this context, our critical infrastructure and key resources (CIKR) may be directly exposed to the events themselves or indirectly exposed as a result of the dependencies and interdependencies among CIKR.

Within the CIKR protection mission area, national priorities must include preventing catastrophic loss of life and managing cascading, disruptive impacts on the U.S. and global economies across multiple threat scenarios. Achieving this goal requires a strategy that appropriately balances resiliency—a traditional American strength in adverse times—with focused, risk-informed prevention, protection, and preparedness activities so that we can manage and reduce the most serious risks that we face.

These concepts represent the pillars of our National Infrastructure Protection Plan (NIPP) and its 18 supporting Sector-Specific Plans (SSPs). The plans are carried out in practice by an integrated network of Federal departments and agencies, State and local government agencies, private sector entities, and a growing number of regional consortia—all operating together within a largely voluntary CIKR protection framework. This multidimensional public-private sector partnership is the key to success in this inherently complex mission area. Building this partnership under the NIPP has been a major accomplishment to date and has facilitated closer cooperation and a trusted relationship in and across the 18 CIKR sectors. Integrating multi-jurisdictional and multi-sector authorities, capabilities, and resources in a unified but flexible approach that can also be tailored to specific sector and regional risk landscapes and operating environments is the path to successfully enhancing our Nation's CIKR protection.

The NIPP meets the requirements that the President set forth in Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection, and provides the overarching approach for integrating the Nation's many CIKR protection initiatives into a single national effort. It sets forth a comprehensive risk management framework and clearly defined roles and responsibilities for

the Department of Homeland Security; Federal Sector-Specific Agencies; and other Federal, State, regional, local, tribal, territorial, and private sector partners implementing the NIPP.

The 2009 NIPP captures the evolution and maturation of the processes and programs first outlined in 2006 and was developed collaboratively with CIKR partners at all levels of government and the private sector. Participation in the implementation of the NIPP provides the government and the private sector with the opportunity to use collective expertise and experience to more clearly define CIKR protection issues and practical solutions and to ensure that existing CIKR protection planning efforts, including business continuity and resiliency planning, are recognized.

I ask for your continued commitment and cooperation in the implementation of both the NIPP and the supporting SSPs so that we can continue to enhance the protection of the Nation's CIKR.

Michael Chertoff

A handwritten signature in black ink, appearing to read "Michael Chertoff". The signature is written in a cursive style with a large, stylized initial "M".



Table of Contents

Preface	i
Executive Summary	1
1. Introduction	7
1.1 Purpose	8
1.2 Scope	9
1.3 Applicability	9
1.3.1 Goal	9
1.3.2 The Value Proposition	10
1.4 Threats to the Nation's CIKR	11
1.4.1 The Vulnerability of the U.S. Infrastructure to 21 st Century Threats and Hazards	11
1.4.2 The Nature of the Terrorist Adversary	11
1.4.3 All-Hazards and CIKR Protection	11
1.5 Special Considerations	12
1.5.1 The Cyber Dimension	12
1.5.2 International CIKR Protection	12
1.6 Achieving the Goal of the NIPP	13
1.6.1 Understanding and Sharing Information	13
1.6.2 Building Partnerships	13
1.6.3 Implementing a CIKR Risk Management Program	13
1.6.4 Maximizing Efficient Use of Resources for CIKR Protection	14
2. Authorities, Roles, and Responsibilities	15
2.1 Authorities	15
2.2 Roles and Responsibilities	16
2.2.1 Department of Homeland Security	16
2.2.2 Sector-Specific Agencies	18
2.2.3 Other Federal Departments, Agencies, and Offices	20
2.2.4 State, Local, Tribal, and Territorial Governments	21
2.2.5 CIKR Owners and Operators	24
2.2.6 Advisory Councils	25
2.2.7 Academia and Research Centers	25

3. The Strategy: Managing Risk	27
3.1 Set Goals and Objectives	28
3.2 Identify Assets, Systems, and Networks	29
3.2.1 National Infrastructure Inventory	29
3.2.2 Protecting and Accessing Inventory Information	30
3.2.3 SSA Role in Inventory Development and Maintenance	31
3.2.4 State and Local Government Role in Inventory Development and Maintenance	31
3.2.5 Identifying Cyber Infrastructure	32
3.2.6 Identifying Positioning, Navigation, and Timing Services	32
3.3 Assess Risks	32
3.3.1 NIPP Core Criteria for Risk Assessments	33
3.3.2 Risk Scenario Identification	34
3.3.3 Consequence Assessment	34
3.3.4 Vulnerability Assessment	36
3.3.5 Threat Assessment	37
3.3.6 Homeland Infrastructure Threat and Risk Analysis Center	38
3.4 Prioritize	40
3.4.1 The Prioritization Process	40
3.4.2 Tailoring Prioritization Approaches to Sector and Decisionmakers' Needs	41
3.4.3 The Uses of Prioritization	42
3.5 Implement Protective Programs and Resiliency Strategies	42
3.5.1 Risk Management Actions	43
3.5.2 Characteristics of Effective Protective Programs and Resiliency Strategies	43
3.5.3 Risk Management Activities, Initiatives, and Reports	44
3.6 Measure Effectiveness	46
3.6.1 NIPP Metrics Types and Progress Indicators	47
3.6.2 Gathering Performance Information	47
3.6.3 Assessing Performance and Reporting on Progress	48
3.7 Using Metrics and Performance Measurement for Continuous Improvement	48
4. Organizing and Partnering for CIKR Protection	49
4.1 Leadership and Coordination Mechanisms	49
4.1.1 National-Level Coordination	50
4.1.2 Sector Partnership Coordination	50
4.1.3 Regional Coordination and the Partnership Model	53
4.1.4 International CIKR Protection Cooperation	53
4.2 Information Sharing: A Network Approach	56
4.2.1 Supporting the CIKR Protection Mission	57

4.2.2	The CIKR Information-Sharing Environment	60
4.2.3	Federal Intelligence Node	61
4.2.4	Federal Infrastructure Node	62
4.2.5	State, Local, Tribal, Territorial, and Regional Node	62
4.2.6	Private Sector Node	62
4.2.7	DHS Operations Node	63
4.2.8	Other Information-Sharing Nodes	65
4.3	Protection of Sensitive CIKR Information	66
4.3.1	Protected Critical Infrastructure Information Program	66
4.3.2	Other Information Protection Protocols	68
4.4	Privacy and Constitutional Freedoms	69
5.	CIKR Protection as Part of the Homeland Security Mission	71
5.1	A Coordinated National Approach to the Homeland Security Mission	71
5.1.1	Legislation	71
5.1.2	Strategies	71
5.1.3	Homeland Security Presidential Directives and National Initiatives	73
5.2	The CIKR Protection Component of the Homeland Security Mission	76
5.3	Relationship of the NIPP and SSPs to Other CIKR Plans and Programs	76
5.3.1	Sector-Specific Plans	76
5.3.2	State, Regional, Local, Tribal, and Territorial CIKR Protection Programs	77
5.3.3	Other Plans or Programs Related to CIKR Protection	77
5.4	CIKR Protection and Incident Management	78
5.4.1	The National Response Framework	78
5.4.2	Transitioning From NIPP Steady-State to Incident Management	78
6.	Ensuring an Effective, Efficient Program Over the Long Term	81
6.1	Building National Awareness	81
6.1.1	Education and Training	82
6.1.2	Core Competencies for Implementing CIKR Protection	83
6.1.3	Individual Education and Training	85
6.1.4	Organizational Training and Exercises	86
6.1.5	CIKR Partner Role and Approach	88
6.2	Conducting Research and Development and Using Technology	88
6.2.1	The SAFETY Act	89
6.2.2	National Critical Infrastructure Protection R&D Plan	90
6.2.3	Other R&D That Supports CIKR Protection	91
6.2.4	DHS Science and Technology Strategic Framework	91
6.2.5	Transitioning Requirements Into Reality	91

6.3 Building, Protecting, and Maintaining Databases, Simulations, and Other Tools	92
6.3.1 National CIKR Protection Data Systems	92
6.3.2 Simulation and Modeling	93
6.3.3 Coordination on Databases and Modeling	94
6.4 Continuously Improving the NIPP and the SSPs	94
6.4.1 Management and Coordination	94
6.4.2 Maintenance and Updates	95
7. Providing Resources for the CIKR Protection Program	97
7.1 The Risk-Informed Resource Allocation Process	97
7.1.1 Sector-Specific Agency Reporting to DHS	98
7.1.2 State Government Reporting to DHS	98
7.1.3 State, Local, Tribal, and Territorial Government Coordinating Council Reporting to DHS	99
7.1.4 Regional Consortium Coordinating Council Reporting to DHS	99
7.1.5 Aggregating Submissions to DHS	99
7.2 Federal Resource Prioritization for DHS, the SSAs, and Other Federal Agencies	100
7.2.1 Department of Homeland Security	100
7.2.2 Sector-Specific Agencies	100
7.2.3 Summary of Roles and Responsibilities	101
7.3 Federal Resources for State and Local Government Preparedness	101
7.3.1 Overarching Homeland Security Grant Programs	101
7.3.2 Targeted Infrastructure Protection Programs	102
7.4 Other Federal Grant Programs That Contribute to CIKR Protection	102
7.5 Setting an Agenda in Collaboration with CIKR Protection Partners	103
List of Acronyms and Abbreviations	105
Glossary of Key Terms	109
Appendixes	
Appendix 1: Special Considerations	113
Appendix 1A: Cross-Sector Cybersecurity	113
Appendix 1B: International CIKR Protection	125
Appendix 2: Summary of Relevant Statutes, Strategies, and Directives	135
Appendix 3: The Protection Program	147
Appendix 3A: NIPP Core Criteria for Risk Assessments	147
Appendix 3B: Existing CIKR Protection Programs and Initiatives	149
Appendix 3C: Infrastructure Data Warehouse	155
Appendix 4: Existing Coordination Mechanisms	159
Appendix 5: Integrating CIKR Protection as Part of the Homeland Security Mission	163
Appendix 5A: State, Local, Tribal, and Territorial Government Considerations	163
Appendix 5B: Recommended Homeland Security Practices for Use by the Private Sector	167
Appendix 6: S&T Plans, Programs, and Research & Development	171

List of Figures and Tables

Figures

Figure S-1: Protection	2
Figure S-2: NIPP Risk Management Framework	4
Figure 1-1: Protection	7
Figure 3-1: NIPP Risk Management Framework	27
Figure 3-2: NIPP Risk Management Framework: Set Goals and Objectives	29
Figure 3-3: NIPP Risk Management Framework: Identify Assets, Systems, and Networks	30
Figure 3-4: NIPP Risk Management Framework: Assess Risks	33
Figure 3-5: NIPP Risk Management Framework: Prioritize	40
Figure 3-6: NIPP Risk Management Framework: Implement Programs	42
Figure 3-7: NIPP Risk Management Framework: Measure Effectiveness	46
Figure 3-8: NIPP Risk Management Framework: Feedback Loop for Continuous Improvement of CIKR Protection	48
Figure 4-1: Sector Partnership Model	50
Figure 4-2: NIPP Networked Information-Sharing Approach	58
Figure 5-1: National Framework for Homeland Security	72
Figure 6-1: Continuum of CIKR Capability Development	82
Figure 6-2: Developing CIKR Core Competencies	83
Figure 6-3: National Exercise Program Tiers	87
Figure 6-4: The NIPP R&D Requirements Generation Process	92
Figure 7-1: National CIKR Protection Annual Report Process	99
Figure 7-2: National CIKR Protection Annual Report Analysis	100
Figure 7-3: DHS and SSA Roles and Responsibilities in Federal Resource Allocation	101

Tables

Table S-1: Sector-Specific Agencies and Assigned CIKR Sectors	3
Table 2-1: Sector-Specific Agencies and Assigned CIKR Sectors	19
Table 6-1: CIKR Competency Areas	84
Table 3C-1: Database Integration	156



Executive Summary

Protecting and ensuring the resiliency of the critical infrastructure and key resources (CIKR) of the United States is essential to the Nation's security, public health and safety, economic vitality, and way of life. Attacks on CIKR could significantly disrupt the functioning of government and business alike and produce cascading effects far beyond the targeted sector and physical location of the incident. Direct terrorist attacks and natural, manmade, or technological hazards could produce catastrophic losses in terms of human casualties, property destruction, and economic effects, as well as profound damage to public morale and confidence. Attacks using components of the Nation's CIKR as weapons of mass destruction could have even more devastating physical and psychological consequences.

1 Introduction

The overarching goal of the National Infrastructure Protection Plan (NIPP) is to:

Build a safer, more secure, and more resilient America by preventing, deterring, neutralizing, or mitigating the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit elements of our Nation's CIKR and to strengthen national preparedness, timely response, and rapid recovery of CIKR in the event of an attack, natural disaster, or other emergency.

The NIPP provides the unifying structure for the integration of existing and future CIKR protection efforts and resiliency strategies into a single national program to achieve this goal. The NIPP framework supports the prioritization of protection and resiliency initiatives and investments across sectors to ensure that government and private sector resources are applied where they offer the most benefit for mitigating risk by lessening vulnerabilities, deterring threats, and minimizing the consequences of terrorist attacks and other manmade and natural disasters. The NIPP risk management framework recognizes and builds on existing public and private sector protective programs and resiliency strategies in order to be cost-effective and to minimize the burden on CIKR owners and operators.

Protection includes actions to mitigate the overall risk to CIKR assets, systems, networks, functions, or their inter-connecting links. In the context of the NIPP, this includes actions to deter the threat, mitigate vulnerabilities, or minimize the consequences associated with a terrorist attack or other incident (see figure S-1). Protection can include a wide range of activities, such as improving security protocols, hardening facilities, building resiliency and redundancy, incorporating hazard resistance into facility design, initiating active or passive countermeasures, installing security systems, leveraging "self-healing" technologies, promoting workforce surety programs, implementing cybersecurity measures, training and exercises, business continuity planning, and restoration and recovery actions, among various others.

Achieving the NIPP goal requires actions to address a series of objectives, which include:

- Understanding and sharing information about terrorist threats and other hazards with CIKR partners;
- Building partnerships to share information and implement CIKR protection programs;

Figure S-1: Protection



- Implementing a long-term risk management program; and
- Maximizing the efficient use of resources for CIKR protection, restoration, and recovery.

These objectives require a collaborative partnership among CIKR partners, including: the Federal Government; State, local, tribal, and territorial governments; regional coalitions; the private sector; international entities; and nongovernmental organizations. The NIPP provides the framework that defines a set of flexible processes and mechanisms that these CIKR partners will use to develop and implement the national program to protect CIKR across all sectors over the long term.

2 Authorities, Roles, and Responsibilities

The Homeland Security Act of 2002 provides the basis for Department of Homeland Security (DHS) responsibilities in the protection of the Nation’s CIKR. The act assigns DHS the responsibility for developing a comprehensive national plan for securing CIKR and for recommending the “measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other agencies of the Federal Government and in cooperation with State and local government agencies and authorities, the private sector, and other entities.”

The national approach for CIKR protection is provided through the unifying framework established in Homeland Security Presidential Directive 7 (HSPD-7). This directive establishes the U.S. policy for “enhancing protection of the Nation’s CIKR” and mandates a national plan to actuate that policy. In HSPD-7, the President designates the Secretary of Homeland Security as the “principal Federal official to lead CIKR protection efforts among Federal departments and agencies, State and local governments, and the private sector” and assigns responsibility for CIKR sectors to Federal Sector-Specific Agencies (SSAs) (see table S-1). It also provides the criteria for establishing or recognizing additional sectors. In

accordance with HSPD-7, the NIPP delineates the roles and responsibilities for partners in carrying out CIKR protection activities while respecting and integrating the authorities, jurisdictions, and prerogatives of these partners.

Primary roles for CIKR partners include:

- **Department of Homeland Security:** Coordinates the Nation’s overall CIKR protection efforts and oversees NIPP development, implementation, and integration with national preparedness initiatives.
- **Sector-Specific Agencies:** Implement the NIPP framework and guidance as tailored to the specific characteristics and risk landscapes of each of the CIKR sectors.
- **Other Federal Departments, Agencies, and Offices:** Implement specific CIKR protection roles designated in HSPD-7 or other relevant statutes, executive orders, and policy directives.
- **State, Local, Tribal, and Territorial Governments:** Develop and implement a CIKR protection program, in accordance with the NIPP risk management framework, as a component of their overarching homeland security programs.
- **Regional Partners:** Use partnerships that cross jurisdictional and sector boundaries to address CIKR protection within a defined geographical area.
- **Boards, Commissions, Authorities, Councils, and Other Entities:** Perform regulatory, advisory, policy, or business oversight functions related to various aspects of CIKR operations and protection within and across sectors and jurisdictions.
- **Private Sector Owners and Operators:** Undertake CIKR protection, restoration, coordination, and cooperation activities, and provide advice, recommendations, and subject matter expertise to all levels of government.
- **Homeland Security Advisory Councils:** Provide advice, recommendations, and expertise to the government regarding protection policy and activities.
- **Academia and Research Centers:** Provide CIKR protection subject matter expertise, independent analysis, research and development (R&D), and educational programs.

3 The CIKR Protection Program Strategy: Managing Risk

The cornerstone of the NIPP is its risk analysis and management framework (see figure S-2) that establishes the processes for combining consequence, vulnerability, and threat information to produce assessments of national or sector

Table S-1: Sector-Specific Agencies and Assigned CIKR Sectors

Sector-Specific Agency	Critical Infrastructure and Key Resources Sector
Department of Agriculture ^a Department of Health and Human Services ^b	Agriculture and Food
Department of Defense ^c	Defense Industrial Base
Department of Energy	Energy ^d
Department of Health and Human Services	Healthcare and Public Health
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Water ^e
Department of Homeland Security <i>Office of Infrastructure Protection</i>	Chemical Commercial Facilities Critical Manufacturing Dams Emergency Services Nuclear Reactors, Materials, and Waste
<i>Office of Cybersecurity and Communications</i>	Information Technology Communications
<i>Transportation Security Administration</i>	Postal and Shipping
<i>Transportation Security Administration United States Coast Guard^f</i>	Transportation Systems ^g
<i>Immigration and Customs Enforcement, Federal Protective Service</i>	Government Facilities ^h

^a The Department of Agriculture is responsible for agriculture and food (meat, poultry, and egg products).

^b The Department of Health and Human Services is responsible for food other than meat, poultry, and egg products.

^c Nothing in this plan impairs or otherwise affects the authority of the Secretary of Defense over the Department of Defense (DoD), including the chain of command for military forces from the President as Commander in Chief, to the Secretary of Defense, to the commander of military forces, or military command and control procedures.

^d The Energy Sector includes the production, refining, storage, and distribution of oil, gas, and electric power, except for commercial nuclear power facilities.

^e The Water Sector includes drinking water and wastewater systems.

^f The U.S. Coast Guard is the SSA for the maritime transportation mode.

^g As stated in HSPD-7, the Department of Transportation and the Department of Homeland Security will collaborate on all matters relating to transportation security and transportation infrastructure protection.

^h The Department of Education is the SSA for the Education Facilities Subsector of the Government Facilities Sector.

risk. The risk management framework is structured to promote continuous improvement to enhance CIKR protection by focusing activities on efforts to: set goals and objectives; identify assets, systems, and networks; assess risk based on consequences, vulnerabilities, and threats; establish priorities based on risk assessments and, increasingly, on return-on-investment for mitigating risk; implement protective programs and resiliency strategies; and measure effectiveness. The results of these processes drive CIKR risk-reduction and management activities. The NIPP risk management framework is tailored to and applied on an asset, system, network, or mission essential function basis, depending on the fundamental characteristics of the individual CIKR sectors. DHS, the SSAs, and other CIKR partners share responsibilities for implementing the risk management framework.

4 Organizing and Partnering for CIKR Protection

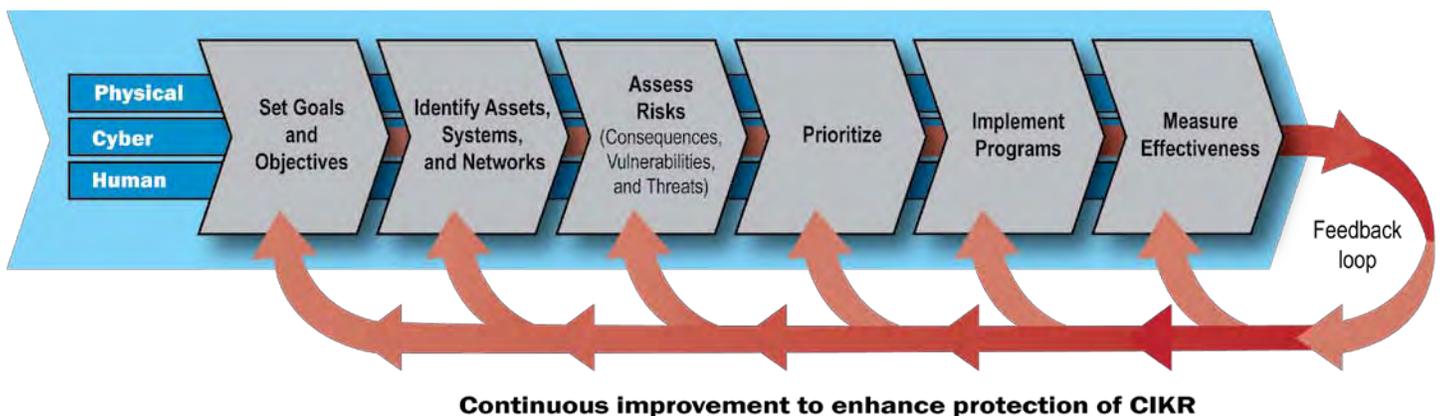
The enormity and complexity of the Nation’s CIKR, the distributed character of our national protective architecture, and the uncertain nature of the terrorist threat and other manmade or natural disasters make the effective implementation of protection and resiliency efforts a great challenge. To be effective, the NIPP must be implemented using organizational structures and partnerships committed to sharing and protecting the information needed to achieve the NIPP goal and supporting objectives.

The NIPP defines the organizational structures that provide the framework for coordination of CIKR protection efforts at all levels of government, as well as within and across sectors. Sector-specific planning and coordination are addressed through coordinating councils that are established for each sector. Sector Coordinating Councils (SCCs) comprise the repre-

sentatives of owners and operators, generally from the private sector. Government Coordinating Councils (GCCs) comprise the representatives of the SSAs; other Federal departments and agencies; and State, local, tribal, and territorial governments. These councils create a structure through which representative groups from all levels of government and the private sector can collaborate or share existing approaches to CIKR protection and work together to advance capabilities. Engaging and coordinating with foreign governments and international organizations are also essential to ensuring the protection and resiliency of U.S. CIKR, both at home and abroad. The NIPP provides the mechanisms and processes necessary to enable DHS, the Department of State, the SSAs, and other partners to strengthen international cooperation to support CIKR protection activities and initiatives.

DHS works with cross-sector entities established to promote coordination, communications, and sharing of best practices across CIKR sectors, jurisdictions, or specifically defined geographical areas. Cross-sector issues are challenging to identify and assess comparatively. Interdependency analysis is often so complex that modeling and simulation capabilities must be brought to bear. Cross-sector issues and interdependencies are addressed among the SCCs through the CIKR Cross-Sector Council, which comprises the leadership of each of the SCCs. The Partnership for Critical Infrastructure Security provides this representation with support from the DHS CIKR Executive Secretariat. Cross-sector issues and interdependencies among the GCCs are addressed through the Government Cross-Sector Council, which comprises the NIPP Federal Senior Leadership Council (FSLC) and the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC). Additionally, the Regional Consortium Coordinating Council (RCCC) provides a forum for those with regionally based interests in CIKR protection.

Figure S-2: NIPP Risk Management Framework



Efficient information-sharing and information-protection processes based on mutually beneficial, trusted relationships help ensure implementation of effective, coordinated, and integrated CIKR protection programs and activities. Information sharing enables both government and private sector partners to assess events accurately, formulate risk assessments, and determine appropriate courses of action. The NIPP uses a network approach to information sharing that represents a new model for how CIKR partners share and protect the information needed to analyze risk and make risk-informed decisions. A network approach enables secure, multidirectional information sharing between and across government and industry. This approach provides mechanisms, using information-protection protocols as required, to support the development and sharing of strategic and specific threat assessments, threat warnings, incident reports, all-hazards consequence assessments, risk assessments, and best practices. This information-sharing approach allows CIKR partners to assess risks, identify and prioritize risk management opportunities, allocate resources, conduct risk management activities, and make continuous improvements to the Nation's CIKR protection posture.

NIPP implementation relies on CIKR information provided voluntarily by owners and operators. Much of this is sensitive business or security information that could cause serious damage to private firms, the economy, public safety, or security through unauthorized disclosure or access. The Federal Government has a statutory responsibility to safeguard CIKR protection-related information. DHS and other Federal agencies use a number of programs and procedures, such as the Protected Critical Infrastructure Information (PCII) Program, to ensure that security-related information is properly safeguarded.

The CIKR protection activities defined in the NIPP are guided by legal requirements such as those described in the Privacy Act of 1974 and are designed to achieve both security and protection of civil rights and liberties.

5 CIKR Protection: An Integral Part of the Homeland Security Mission

The NIPP defines the CIKR protection component of the homeland security mission. Implementing CIKR protection requires partnerships, coordination, and collaboration among all levels of government and the private sector. To enable this, the NIPP provides guidance on the structure and content of each sector's CIKR plan, as well as the CIKR protection-related aspects of State and local homeland security plans. This

provides a baseline framework that informs the flexible and tailored development, implementation, and updating of Sector-Specific Plans; State and local homeland security strategies; and partner CIKR protection programs and resiliency strategies.

To be effective, the NIPP must complement other plans designed to help prevent, prepare for, protect against, respond to, and recover from terrorist attacks, natural disasters, and other emergencies. Homeland security plans and strategies at the Federal, State, local, tribal, and territorial levels of government address CIKR protection within their respective jurisdictions. Similarly, CIKR owners and operators have responded to the increased threat environment by instituting a range of CIKR protection-related plans and programs, including business continuity and resilience and response measures. Implementation of the NIPP is coordinated among CIKR partners to ensure that it does not result in the creation of duplicative or costly risk management requirements that offer little enhancement of CIKR protection.

The NIPP, the National Preparedness Guidelines (NPG), and the National Response Framework (NRF) together provide a comprehensive, integrated approach to the homeland security mission. The NIPP establishes the overall risk-informed approach that defines the Nation's CIKR protection posture, while the NRF provides the approach for domestic incident management. The NPG sets forth national priorities, doctrine, and roles and responsibilities for building capabilities across the prevention, protection, response, and recovery mission areas. Increases in CIKR protective measures in the context of specific threats or that correspond to the threat conditions established in the Homeland Security Advisory System (HSAS) provide an important bridge between NIPP steady-state protection and the incident management activities under the NRF.

The NRF is implemented to guide overall coordination of domestic incident management activities. NIPP partnerships and processes provide the foundation for the CIKR dimension of the NRF, facilitating threat and incident management across a spectrum of activities, including incident prevention, response, and recovery. The NPG is implemented through the application of target capabilities during the course of assessment, planning, training, exercises, grants, and technical assistance activities. Implementation of the NIPP is both a national preparedness priority and a framework with which to achieve protection capabilities as defined by the NPG.

6 Ensuring an Effective, Efficient Program Over the Long Term

To ensure an effective, efficient CIKR protection program over the long term, the NIPP relies on the following mechanisms:

- Building national awareness to support the CIKR protection program, related protection investments, and protection activities by ensuring a focused understanding of all hazards and of what is being done to protect and enable the timely restoration of the Nation's CIKR in light of such threats;
- Enabling education, training, and exercise programs to ensure that skilled and knowledgeable professionals and experienced organizations are able to undertake NIPP-related responsibilities in the future;
- Conducting research and development and using technology to improve CIKR protection-related capabilities or to lower the costs of existing capabilities so that CIKR partners can afford to do more with limited budgets;
- Developing, safeguarding, and maintaining data systems and simulations to enable continuously refined risk assessment within and across sectors and to ensure preparedness for incident management; and
- Continuously improving the NIPP and associated plans and programs through ongoing review and revision, as required.

7 Providing Resources for the CIKR Protection Program

Chapter 7 describes an integrated, risk-informed approach used to: establish priorities, determine requirements, and guide resource support for the national CIKR protection program; focus Federal grant assistance to State, local, tribal, and territorial entities; and complement relevant private sector activities. At the Federal level, DHS provides recommendations regarding CIKR protection priorities and requirements to the Executive Office of the President through the National CIKR Protection Annual Report. This report is based on information about priorities, requirements, and related program funding information that is submitted to DHS by the SSA of each sector, the SLTTGCC, and the RCCC as assessed in the context of the National Risk Profile and national priorities. The process for allocating Federal resources through grants to State, local, and tribal governments uses a similar approach. DHS aggregates information regarding State, local, tribal, and territorial CIKR protection priorities and requirements. DHS uses these data to inform the establishment of

national priorities for CIKR protection and to help ensure that resources are prioritized for protective programs that have the greatest potential for mitigating risk. This risk-informed approach also includes mechanisms to involve private sector partners in the planning process and supports collaboration among CIKR partners to establish priorities, define requirements, share information, and maximize risk reduction.

1. Introduction

Protecting and ensuring the continuity of the critical infrastructure and key resources (CIKR) of the United States is essential to the Nation's security, public health and safety, economic vitality, and way of life. CIKR includes systems and assets, whether physical or virtual, so vital to the United States that the incapacitation or destruction of such systems and assets would have a debilitating impact on national security, national economic security, public health or safety, or any combination of those matters. Terrorist attacks on our CIKR, as well as other manmade or natural disasters, could significantly disrupt the functioning of government and business alike and produce cascading effects far beyond the affected CIKR and physical location of the incident. Direct and indirect impacts could result in large-scale human casualties, property destruction, economic disruption, and mission failure, and also significantly damage national morale and public confidence. Terrorist attacks using components of the Nation's CIKR as weapons of mass destruction (WMD)¹ could have even more devastating physical, psychological, and economic consequences.

Protecting the Nation's CIKR is essential to making America safer, more secure, and more resilient in the context of terrorist attacks and other natural and manmade hazards.

Protection includes actions to mitigate the overall risk to CIKR assets, systems, networks, functions, or their interconnecting links resulting from exposure, injury, destruction, incapacitation, or exploitation. In the context of the National Infrastructure Protection Plan (NIPP), this includes actions to deter the threat, mitigate vulnerabilities, or minimize the consequences associated with a terrorist attack or other manmade or natural disaster (see figure 1-1). Protection can include a wide range of activities such as improving security protocols, hardening facilities, building resiliency and redundancy, incorporating hazard resistance into facility design, initiating active or passive countermeasures, installing security systems, leveraging "self-healing" technologies, promoting workforce surety programs, implementing cybersecurity measures, training and exercises, and business continuity planning, among others. The NIPP (June 2006; revised January 2009) and its complementary Sector-Specific Plans (SSPs) (May 2007; to be reissued in 2010) provide a

Figure 1-1: Protection



¹ (1) Any explosive, incendiary, or poison gas (i) bomb, (ii) grenade, (iii) rocket having a propellant charge of more than 4 ounces, (iv) missile having an explosive or incendiary charge of more than one-quarter ounce, (v) mine, or (vi) similar device; (2) any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors; (3) any weapon involving a disease organism; or (4) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life (18 U.S.C. 2332a).

consistent, unifying structure for integrating both existing and future CIKR protection efforts. The NIPP also provides the core coordinating processes and mechanisms that enable all levels of government and private sector partners to work together to implement CIKR protection in an effective and efficient manner.

The NIPP was developed through extensive coordination with partners at all levels of government and the private sector. NIPP processes are designed to be adapted and tailored to individual sector and partner requirements, including State, local, or regional issues. Participation in the implementation of the NIPP provides government and the private sector with the opportunity to use collective expertise and experience to more clearly define issues and solutions, and to ensure that existing CIKR protection approaches and efforts, including business continuity and resiliency planning, are recognized.

Since the NIPP and the SSPs were first released, the processes and programs outlined in those documents have continued to evolve and mature. This update to the NIPP reflects many advances, including:

- The issuance of the SSPs, which followed the release of the NIPP;
- Establishment of Critical Manufacturing as the 18th CIKR sector and the designation of Education as a subsector of Government Facilities;
- Expansion of the sector partnership model to include the geographically focused Regional Consortium Coordinating Council (RCCC);
- CIKR mission integration within State and local fusion centers;
- Evolution of the National Asset Database to the Infrastructure Information Collection System and the Infrastructure Data Warehouse;
- Developments in the programs, approaches, and tools used to implement the NIPP risk management framework;
- Updates on risk methodologies, information-sharing mechanisms, and other CIKR protection programs;
- Inclusion of outcome-focused performance measurement and reporting processes;
- Description of additional Homeland Security Presidential Directives, national strategies, and legislation;

- Release of the Chemical Facility Anti-Terrorism Standards (CFATS), establishing a regulatory framework for those industries that involve the production, use, and storage of high-risk chemicals;
- Discussion of expanded CIKR protection-related education, training, outreach, and exercise programs;
- Evolution from the National Response Plan to the National Response Framework (NRF); and
- Inclusion of further information on research and development (R&D) and modeling, simulation, and analysis processes and initiatives.

Additionally, the revised NIPP integrates the concepts of resiliency and protection, and broadens the focus of NIPP-related programs and activities to an all-hazards environment.

1.1 Purpose

The NIPP provides the framework for the unprecedented cooperation that is needed to develop, implement, and maintain a coordinated national effort to bring together government at all levels, the private sector, nongovernmental organizations, and international partners. The NIPP depends on supporting SSPs for full implementation of this framework within and across CIKR sectors. SSPs are developed by the Federal Sector-Specific Agencies (SSAs) designated in Homeland Security Presidential Directive 7 (HSPD-7) in close collaboration with sector partners.

Together, the NIPP and SSPs provide the mechanisms for: identifying critical assets, systems, and networks, and their associated functions; understanding threats to CIKR; identifying and assessing vulnerabilities and consequences; prioritizing protection initiatives and investments based on costs and benefits so that they are applied where they offer the greatest mitigation of risk; and enhancing information-sharing mechanisms and protection and resiliency within and across CIKR sectors. The NIPP and SSPs will evolve along with changes to the Nation's CIKR and the risk environment, as well as evolving strategies and technologies for protecting against and responding to threats and incidents. Implementation of the NIPP and the SSPs occurs at all levels through actions taken by: Federal agencies; State, regional, local, tribal, and territorial governments and organizations; and individual CIKR owners and operators.

1.2 Scope

The NIPP considers a full range of physical, cyber, and human risk elements within and across sectors. In accordance with the policy direction established in HSPD-7, the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, and the National Strategy to Secure Cyberspace, the NIPP includes a special focus on the unique and potentially catastrophic impact of terrorist attacks. At the same time, the NIPP builds on and is structured to be consistent with and supportive of the Nation's all-hazards approach to homeland security preparedness and domestic incident management. Many of the benefits of enhanced CIKR protection are most sustainable when protective programs and resiliency strategies are designed to address all hazards.

The NIPP addresses ongoing and future activities within each of the CIKR sectors identified in HSPD-7 and across the sectors regionally, nationally, and within individual States or communities. It defines processes and mechanisms used to prioritize protection of U.S. CIKR (including territories and territorial seas) and to address the interconnected global networks upon which the Nation's CIKR depend. The processes outlined in the NIPP and the SSPs recognize that protective measures do not end at a facility's fence or at a national border, and are often a component of a larger business continuity approach. Also considered are the implications of cross-border infrastructures, international vulnerabilities, and cross-sector dependencies and interdependencies.

1.3 Applicability

The NIPP is applicable to a wide array of public and private sector CIKR partners in different ways. The framework generally is applicable to all partners with CIKR protection responsibilities and includes explicit roles and responsibilities for the Federal Government, including CIKR under the control of independent regulatory agencies, and the legislative, executive, and judicial branches. Federal departments and agencies with specific responsibilities for CIKR protection are required to take actions that are consistent with HSPD-7. The NIPP also provides an organizing structure, guidelines, and recommended activities for other partners to help ensure consistent implementation of the national framework and

the most effective use of resources. State,² local,³ tribal, and territorial government partners are required to establish CIKR protection programs that are consistent with the National Preparedness Guidelines and as a condition of eligibility for certain Federal grant programs.

Owners and operators are encouraged to participate in the NIPP partnership and to initiate measures to augment existing plans for risk management, resiliency, business continuity, and incident management and emergency response in line with the NIPP framework.

1.3.1 Goal

The overarching goal of the NIPP is to:

Build a safer, more secure, and more resilient America by preventing, deterring, neutralizing, or mitigating the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit elements of our Nation's CIKR, and to strengthen national preparedness, timely response, and rapid recovery of CIKR in the event of an attack, natural disaster, or other emergency.

Achieving this goal requires understanding and sharing information about terrorist threats and other hazards, building partnerships, implementing a long-term risk management program, and maximizing the efficient use of resources. Measuring progress toward achieving the NIPP goal requires that CIKR partners strive toward:

- Coordinated CIKR risk management plans and programs that are in place to address known and potential threats and hazards;
- Structures and processes that are flexible and adaptable both to incorporate operational lessons learned and best practices, and also to quickly reflect a changing threat or incident environment;
- Processes in place to identify and address dependencies and interdependencies to allow for more timely and effective implementation of short-term protective actions and more rapid response and recovery; and
- Access to robust information-sharing networks that include relevant intelligence and threat analysis, and real-time incident reporting.

² Consistent with the definition of "State" in the Homeland Security Act of 2002, all references to States within the NIPP are applicable to the territories and include by reference any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States (Homeland Security Act).

³ A county, municipality, city, town, township, local public authority, school district, special district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government; an Indian tribe or authorized tribal organization, or, in Alaska, a Native village or Alaska Regional Native Corporation; and a rural community, unincorporated town or village, or other public entity (Homeland Security Act).

1.3.2 The Value Proposition

The public-private partnership called for in the NIPP provides the foundation for effective CIKR protection. Prevention, response, mitigation, and recovery efforts are most efficient and effective when there is the full participation of government and industry partners; the mission suffers (e.g., full benefits are not realized) without the robust participation of a wide array of CIKR partners.

The success of the NIPP partnership depends on articulating the benefits to government and the private sector partners. Industry capabilities that add value to the government include:

- Understanding of CIKR assets, systems, networks, and facilities, and other capabilities through industry ownership and management of a vast majority of CIKR in most sectors;
- Ability to take action to reduce risk and to respond to and recover from incidents;
- Ability to innovate and to provide products, services, and technologies to quickly focus on mission needs; and
- Robust relationships that are useful for sharing and protecting sensitive information regarding threats, vulnerabilities, countermeasures, and best practices.

Although articulating the value proposition to the government typically is easier to achieve, it is often more difficult to articulate the direct benefits of participation for the private sector. In assessing the value proposition for the private sector, there is a clear national interest in ensuring the collective protection and resiliency of the Nation's CIKR. More specific benefits that have been realized during the first few years of the partnership include:

- Participation in both a policy development and risk analysis and management framework that helps focus both corporate and government planning and resource investment;
- Greater information sharing regarding specific threats and hazards enabled by the issuance of security clearances to private sector partners;
- Leveraged application of preparedness guidelines and self-assessment tools within and across sectors so that risks can be managed more effectively and efficiently from the corporate level down to the individual facility level;
- Targeted application of limited resources to the highest risk issues, to include Federal grant funding where appropriate;
- Coordination and planning across multiple agencies for those assets and facilities that are considered to be at the greatest risk;

- Joint R&D and modeling, simulation, and analysis programs;
- Participation in national-level and cross-sector training and exercise programs, as well as the National Incident Management System;
- Access and input into cross-sector interdependency analyses;
- Established informal networks among private sector partners and between the private sector and the various Federal agencies that can be used for all-hazards planning and response; and
- Identification of potential improvements in regulations.

Government can encourage industry to go beyond efforts already justified by their corporate business needs to assist in broad-scale CIKR protection through activities such as:

- Providing owners and operators with timely, accurate, and useful analysis and information on threats to CIKR;
- Ensuring that industry is engaged as early as possible in the development of policies and initiatives related to NIPP implementation;
- Articulating to corporate leaders, through the use of public platforms and private communications, both the business and national security benefits of investing in security measures that exceed their business case;
- Creating an environment that encourages and supports incentives and recognition for companies to voluntarily adopt widely accepted security practices;
- Working with industry to develop and clearly prioritize key missions and enable the protection and/or restoration of related CIKR;
- Providing support for R&D initiatives that is needed to enhance future CIKR protection efforts;
- Providing the resources to enable cross-sector interdependency studies; exercises, symposiums, training sessions, and computer modeling; and otherwise support business continuity planning; and
- Enabling time-sensitive information sharing and restoration and recovery support to priority CIKR facilities and services during emerging threat and incident management situations.

The above examples illustrate some of the ways in which the government can partner with the private sector to add value to industry's ability to assess risk and refine its own business continuity and security plans, as well as to contribute to the security and sustained economic vitality of the Nation.

1.4 Threats to the Nation's CIKR

Presidential guidance and national strategies issued in the aftermath of the September 11, 2001, attacks focused initial CIKR protection efforts on addressing the terrorist threat environment. These new challenges required approaches that focused on intelligence-driven analyses, information sharing, and unprecedented partnerships between the government and the private sector at all levels. The Nation's CIKR owners and operators have decades of experience planning for and responding to natural disasters, industrial accidents, and the deliberate acts of malicious individuals in order to maintain business continuity. However, such plans and preparedness efforts must continue to adapt to a dynamic threat environment and to address vulnerabilities and gaps in CIKR protection in an all-hazards context.

1.4.1 The Vulnerability of the U.S. Infrastructure to 21st Century Threats and Hazards

America is an open, technologically sophisticated, highly interconnected, and complex Nation with a wide array of infrastructure that spans important aspects of the U.S. Government, economy, and society. The vast majority of the CIKR-related assets, systems, and networks are owned and operated by the private sector. However, in sectors such as Water and Government Facilities, the majority of owners and operators are governmental or quasi-governmental entities. The great diversity and redundancy of the Nation's CIKR provide for significant physical and economic resilience in the face of terrorist attacks, natural disasters, or other emergencies, and contribute to the strength of the Nation's economy. However, this vast and diverse aggregation of highly interconnected assets, systems, and networks may also present an attractive array of targets to domestic and international terrorists and magnify greatly the potential for cascading failure in the wake of catastrophic natural or manmade disasters. Improvements in protection and resilience that focus on elements of CIKR that are deemed to be nationally critical can make it more difficult for terrorists to launch destructive attacks, as well as lessen the impact of any attack or other disaster that does occur and provide greater resiliency in response and recovery.

1.4.2 The Nature of the Terrorist Adversary

The number and high profile of international and domestic terrorist attacks and disrupted plots during the last two decades underscore the determination and persistence of terrorist organizations. Terrorists have proven to be relentless, patient, opportunistic, and flexible, learning from experience and

modifying tactics and targets to exploit perceived vulnerabilities and avoid observed strengths. Analysis of terrorist goals and motivations points to domestic and international CIKR as potentially prime targets for terrorist attacks. As security measures around more predictable targets increase, terrorists are likely to shift their focus to less protected targets. Enhancing countermeasures to address any one terrorist tactic or target may increase the likelihood that terrorists will shift to another, which underscores the necessity for a balanced, comparative approach that focuses on managing risk commensurately across all sectors and scenarios of concern.

Terrorist organizations have shown an understanding of the potential consequences of carefully planned attacks on economic, transportation, and symbolic targets, both within the United States and abroad. Future terrorist attacks against CIKR located inside the United States and those located abroad could seriously threaten national security, result in mass casualties, weaken the economy, and damage public morale and confidence.

The NIPP considers a broad range of terrorist objectives, intentions, and capabilities to assess the threat to various components of the Nation's CIKR. Terrorists may contemplate attacks against the Nation's CIKR to achieve direct or indirect effects, or to exploit the infrastructure to cause catastrophic loss of life or economic disruptions.

The NIPP outlines the ways in which the Department of Homeland Security (DHS) and its partners use threat analysis to inform comprehensive risk assessments and risk-mitigation activities. The risk management framework discussed in chapter 3 strikes a balance between ways to mitigate specific threats and general threats. It ensures that the range of risk scenarios considered is broad enough to avoid a "failure of imagination," yet provides a process to enable risk assessment sufficient for the purpose of formulating action plans and programs to enhance resiliency, reduce vulnerability, deter threats, and mitigate potential consequences.

1.4.3 All-Hazards and CIKR Protection

In addition to addressing CIKR protection related to terrorist threats, the NIPP also describes activities relevant to CIKR protection and preparedness in an all-hazards context. The direct impact, disruption, and cascading effects of natural disasters (e.g., Hurricanes Katrina and Rita, the Northridge earthquake, the 2008 Mississippi River floods) and manmade incidents (e.g., the Minneapolis I-35 bridge collapse or the Exxon Valdez oil spill) are documented and underscore the vulnerabilities and interdependencies of the Nation's CIKR.

Many owners and operators, government emergency managers, and first-responders have developed strategies, plans, policies, and procedures to prepare for, mitigate, respond to, and recover from a variety of natural and manmade incidents. The NIPP framework supports these efforts and, additionally, provides an augmented focus on the protection of America's CIKR against terrorist attacks. In fact, the day-to-day public-private coordination structures, information-sharing networks, and risk management frameworks used to implement NIPP steady-state CIKR protection efforts continue to function and provide the CIKR protection dimension for incident management under the National Response Framework (NRF). Likewise, the mitigation and business continuity practices employed to protect against natural hazards and other non-terrorist attacks should support and augment the goals of the NIPP. The NIPP, and the public and private sector partnership that it represents, work in conjunction with other plans and initiatives to provide a strong foundation for preparedness in an all-hazards context.

1.5 Special Considerations

CIKR protection planning involves special consideration for unique cyber elements that support CIKR operations and complex international relationships—two areas of recent focus and attention.

1.5.1 The Cyber Dimension

- The U.S. economy and national security depend greatly and increasingly on the global cyber infrastructure. Cyber infrastructure enables all sectors' functions and services, resulting in a highly interconnected and interdependent global network of CIKR.
- A spectrum of malicious actors routinely conducts attacks against the cyber infrastructure using cyber attack tools. Because of the interconnected nature of the cyber infrastructure, these attacks could spread quickly and have a debilitating effect.
- Cybersecurity includes preventing damage to, unauthorized use of, or exploitation of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. Cybersecurity also includes restoring electronic information and communications systems in the event of a terrorist attack or natural disaster.
- The use of innovative technology and interconnected networks in operations improves productivity and efficiency, but also increases the Nation's vulnerability to cyber threats if cybersecurity is not addressed and integrated appropriately.

Cyber infrastructure includes electronic information and communication systems, and the information contained in these systems. Computer systems, control systems such as Supervisory Control and Data Acquisition (SCADA) systems, and networks such as the Internet are all part of cyber infrastructure.

Information and communications systems are composed of hardware and software that process, store, and communicate data of all types. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information.

Information Technology (IT) critical functions are sets of processes that produce, provide, and maintain products and services. IT critical functions encompass the full set of processes (e.g., R&D, manufacturing, distribution, upgrades, and maintenance) involved in transforming supply inputs into IT products and services.

- The interconnected and interdependent nature of the Nation's CIKR makes it problematic to address the protection of physical and cyber assets independently.
- The NIPP addresses reducing cyber risk and enhancing cybersecurity in two ways: (1) as a cross-sector cyber element that involves DHS, SSAs and Government Coordinating Councils (GCCs), and private sector owners and operators; and (2) as a major component of the Information Technology Sector's responsibility in partnership with the Communications Sector.

1.5.2 International CIKR Protection

- The NIPP addresses international CIKR protection, including interdependencies and vulnerabilities based on threats (and associated consequences) that originate outside the country or pass through it.
- The Federal Government and the private sector work with foreign governments and international/multinational organizations to enhance the confidentiality, integrity, and availability of cyber infrastructure and products.
- Protection of assets, systems, and networks that operate across or near the borders with Canada and Mexico, or rely on other international aspects to enable critical functionality, requires coordination with and planning and/or sharing resources among neighboring governments at all levels, as well as private sector CIKR owners and operators.
- The Federal Government and private sector corporations have a significant number of facilities located outside the United States that may be considered CIKR.

- Special consideration may be required when CIKR is extensively integrated into an international or global market (e.g., financial services, agriculture, energy, transportation, telecommunications, or information technology) or when a sector relies on inputs that are not within the control of U.S. entities.
- Special consideration is required when government facilities and functions are directly affected by foreign-owned and -operated commercial facilities.
- The Federal Government, working in close coordination and cooperation with the private sector, launched the Critical Foreign Dependencies Initiative in 2007 to identify assets and systems located outside the United States, which, if disrupted or destroyed, would critically affect public health and safety, the economy, or national security. The resulting strategic compendium guides engagement with foreign countries in the CIKR protection mission area.

1.6 Achieving the Goal of the NIPP

Achieving the NIPP goal of building a safer, more secure, and more resilient America requires actions that address the following principal objectives:

- Understanding and sharing information about terrorist threats and other hazards;
- Building partnerships to share information and implement CIKR protection and resiliency programs;
- Implementing a long-term risk management program that includes:
 - Hardening, distributing, diversifying, and otherwise ensuring the resiliency of CIKR against known threats and hazards, as well as other potential contingencies;
 - Developing processes to interdict human threats to prevent potential attacks;
 - Planning for rapid response to CIKR disruptions to limit the impact on public health and safety, the economy, and government functions; and
 - Planning for rapid CIKR recovery for those events that are not preventable; and
- Maximizing the efficient use of resources for CIKR protection.

This section provides a summary of the actions needed to address these objectives. More detailed discussions of these actions are included in the chapters that follow.

1.6.1 Understanding and Sharing Information

One of the essential elements needed to achieve the Nation's CIKR protection goals is to ensure the availability and flow of accurate, timely, and relevant information and/or intelligence about terrorist threats and other hazards, information analysis, and incident reporting. This includes:

- Establishing effective information-sharing processes and protocols among CIKR partners;
- Providing intelligence and information to SSAs and other CIKR sector partners as permitted by law;
- Analyzing, warehousing, and sharing risk assessment data in a secure manner that is consistent with relevant legal requirements and information protection responsibilities;
- Providing protocols for real-time threat and incident reporting, alert, and warning; and
- Providing protocols for the protection of sensitive information.

Chapter 3 details the risk and threat analysis processes and products aimed at better understanding and characterizing terrorist threats. Chapter 4 describes the NIPP network approach to information sharing and the process for protecting sensitive CIKR-related information.

1.6.2 Building Partnerships

Building partnerships represents the foundation of the national CIKR protection effort. These partnerships provide a framework to:

- Exchange ideas, approaches, and best practices;
- Facilitate security planning and resource allocation;
- Establish effective coordinating structures among partners;
- Enhance coordination with the international community; and
- Build public awareness.

Chapters 2 and 4 describe partners' roles and responsibilities related to CIKR protection, as well as specific mechanisms for the governance, coordination, and information sharing necessary to enable effective partnerships.

1.6.3 Implementing a CIKR Risk Management Program

The risk management program detailed in the NIPP includes processes to:

- Establish a risk management framework to guide CIKR protection and resiliency programs and activities;
- Take appropriate risk management actions to enhance CIKR protection and resiliency based on all-hazards risk assessments;
- Conduct and update risk assessments, as appropriate, at the asset, system, network, sector, cross-sector, regional, national, and international levels;
- Develop and deploy new technologies to enable more effective and efficient CIKR protection; and
- Provide a system for measurement and improvement of CIKR protection, including:
 - Establishing performance metrics to track the effectiveness of protection programs and resiliency strategies; and
 - Updating the NIPP and SSPs as required.
- Helps align Federal resources with the CIKR protection mission and supports the tracking and accountability of public funds;
- Considers State, local, tribal, and territorial government and private sector issues related to planning, programming, and budgeting;
- Draws on expertise across organizational and national boundaries;
- Shares expertise and speeds implementation of best practices;
- Recognizes the need to build a business case to support further private sector CIKR protection investments; and
- Identifies potential incentives for preparedness and security-related activities where they do not naturally exist in the marketplace.

The NIPP also specifies the processes, initiatives, and milestones necessary to implement an effective long-term CIKR risk management program. Chapter 3 provides details regarding the NIPP risk management framework and the measurement and analysis processes that support its continuous improvement; chapter 6 addresses issues that are important for sustaining and improving CIKR protection over the long term.

1.6.4 Maximizing Efficient Use of Resources for CIKR Protection

Maximizing the efficient use of resources for CIKR protection includes a coordinated and integrated annual process for program implementation that:

- Supports prioritization of programs and activities within and across sectors considering sector needs and requirements;
- Informs the annual Federal process regarding planning, programming, and budgeting for national-level CIKR protection;

Chapter 5 explains how a coordinated national approach to the CIKR protection mission supports the efficient application of resources. Efficient use of resources enables the continuous improvement of the technology, databases, data systems, and other approaches used to protect CIKR and manage risk. These processes are detailed in chapter 6. Chapter 7 describes the annual processes that reflect coordination with SSAs and other partners regarding resource prioritization and allocation. Also discussed are processes to target grants and other funding authorities to maximize and focus the use of resources to support national and sector priorities.

More information about the NIPP is available on the Internet at: www.dhs.gov/nipp or by contacting DHS at: nipp@dhs.gov

2. Authorities, Roles, and Responsibilities

Improving the all-hazards protection and resilience of the Nation's CIKR necessitates: a comprehensive, unifying organization; defined roles and responsibilities; and close cooperation across all levels of government and the private sector. Protection authorities, requirements, resources, capabilities, and risk landscapes vary widely across governmental jurisdictions, sectors, and individual industries and enterprises. This reality presents a complex set of challenges in terms of implementing NIPP programs and measuring performance. Hence, successful implementation of the NIPP and the supporting SSPs depends on an effective partnership framework that: fosters integrated, collaborative engagement and interaction; divides responsibilities among diverse Federal, State, regional, local, tribal, territorial, and private sector partners; and helps to efficiently target the Nation's protection resources based on risk and need.

This chapter includes a brief overview of the relevant authorities and outlines the principal roles and responsibilities of: DHS; SSAs and GCCs; NIPP partners at all levels of government and in the private sector; CIKR owners and operators; and other partners who share responsibility in protecting the Nation's CIKR. A comprehensive understanding of these roles and responsibilities provides the foundation for an effective and sustainable national CIKR protection effort.

2.1 Authorities

The roles and responsibilities described in this chapter are derived from a series of authorities, including the Homeland Security Act of 2002, as well as other CIKR protection-related legislation, Executive Orders, Homeland Security Presidential Directives, and national strategies. The National Strategy for Homeland Security established the national CIKR vision with a charge to “forge an unprecedented level of cooperation throughout all levels of government, with private industry and institutions, and with the American people to protect our critical infrastructures and key assets from terrorist attack.”⁴

HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection, provided the direction to implement this vision. More detailed information on these and other CIKR protection-related authorities is included in chapter 5 and appendix 2A.

The Homeland Security Act provides the primary authority for the overall homeland security mission and outlines DHS responsibilities in the protection of the Nation's CIKR. It established the DHS mission, including “reducing the Nation's vulnerability to terrorist attacks,” major disasters, and other emergencies, and charged the department with evaluating vulnerabilities and ensuring that steps are implemented to protect the high-risk elements of America's CIKR, including food and water systems, agriculture, healthcare systems, emergency services, information technology, communications, banking and finance, energy (electrical, nuclear, gas and oil, and dams), transportation (air, highways, rail, ports, and waterways), the chemical and defense industries, postal and shipping entities, and national monuments and icons. Title II, section 201, of the act assigned primary responsibility to DHS to develop a comprehensive

⁴ The National Strategy for Homeland Security uses the term “key assets,” defined as individual targets whose destruction would not endanger vital systems, but could create a local disaster or profoundly damage the Nation's morale or confidence. The Homeland Security Act and HSPD-7 use the term “key resources,” defined more generally to capture publicly or privately controlled resources essential to the minimal operations of the economy or government. “Key resources” is the current terminology.

national plan for securing CIKR and for recommending “the measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other agencies of the Federal Government and in cooperation with State and local government agencies and authorities, the private sector, and other entities.”

A number of other statutes provide specific legal authorities for both cross-sector and sector-specific CIKR protection and resiliency programs. Examples include the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, which was intended to improve the ability of the United States to prevent, prepare for, and respond to acts of bioterrorism and other public health emergencies; the Maritime Transportation Security Act; the Aviation Transportation Security Act of 2001; the Energy Policy and Conservation Act; the Critical Infrastructure Information Act; the Federal Information Security Management Act; Implementing Recommendations of the 9/11 Commission Act of 2007; and various others.

Many different HSPDs are also relevant to CIKR protection, including, but not limited to:

- HSPD-3, Homeland Security Advisory System
- HSPD-5, Management of Domestic Incidents
- HSPD-8, National Preparedness
- HSPD-9, Defense of the United States Agriculture and Food
- HSPD-10, Biodefense for the 21st Century
- HSPD-19, Combating Terrorist Use of Explosives in the United States
- HSPD-20, National Continuity Policy
- HSPD-22, Domestic Chemical Defense

These separate authorities and directives are tied together as part of the national approach for CIKR protection through the unifying framework established in HSPD-7. HSPD-7, issued in December 2003, established the U.S. policy for “enhancing protection of the Nation’s CIKR.” HSPD-7 establishes a framework for public and private sector partners to identify, prioritize, and protect the Nation’s CIKR from terrorist attacks, with an emphasis on protecting against catastrophic health effects and mass casualties. The directive sets forth the roles and responsibilities for: DHS; SSAs; other Federal departments and agencies; State, local, tribal, and territorial governments; regional partners; the private sector; and other CIKR partners. The following sections address the roles and responsibilities under this integrated approach.

2.2 Roles and Responsibilities

Given the fact that terrorist attacks and certain natural or manmade disasters can have a national-level impact, it is incumbent upon the Federal Government to provide leadership and coordination in the CIKR protection mission area.

2.2.1 Department of Homeland Security

Under HSPD-7, DHS is responsible for leading, integrating, and coordinating the overall national effort to enhance CIKR protection, including collaboratively developing the NIPP and supporting SSPs; developing and implementing comprehensive, multi-tiered risk management programs and methodologies; developing cross-sector and cross-jurisdictional protection guidance, guidelines, and protocols; and recommending risk management and performance criteria and metrics within and across sectors. Per HSPD-7, DHS is also a focal point for the security of cyberspace. HSPD-7 establishes a central source for coordinating best practices and supporting protective programs across and within government agencies. In the directive, the President designates the Secretary of Homeland Security as the “principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources.” The Secretary of Homeland Security is responsible for addressing the complexities of the Nation’s Federal system of government and its multifaceted and interdependent economy, as well as for establishing structures to enhance the close cooperation between the private sector and government at all levels to initiate and sustain an effective CIKR protection program.

In addition to these overarching leadership and cross-sector responsibilities, DHS and its component agencies serve as the SSAs for 11 of the CIKR sectors identified in HSPD-7 or subsequently established using the criteria set forth in HSPD-7: Information Technology; Communications; Transportation Systems; Chemical; Emergency Services; Nuclear Reactors, Materials, and Waste; Postal and Shipping; Dams; Critical Manufacturing; Government Facilities; and Commercial Facilities. Specific SSA responsibilities, as appropriate, are discussed in section 2.2.2. DHS, in the person of the Assistant Secretary for Infrastructure Protection or his/her designee, serves as the co-chair of each of the GCCs with the respective Federal SSA for that sector.

Additional DHS CIKR protection roles and responsibilities include:

- Identifying, prioritizing, and coordinating Federal action in support of the protection of nationally critical assets, systems, and networks, with a particular focus on CIKR that could be exploited to cause catastrophic health effects or mass casualties comparable to those produced by a WMD;
- Coordinating, facilitating, and supporting the overall process for building partnerships and leveraging sector-specific security expertise, relationships, and resources across CIKR sectors, including oversight and support of the sector partnership model described in chapter 4; cooperating with Federal, State, local, tribal, territorial, and regional partners; and collaborating with the Department of State to reach out to foreign governments and international organizations to strengthen the protection of U.S. CIKR;
- Supporting the formation and development of regional partnerships, including promoting new partnerships, enabling information sharing, and sponsoring security clearances;
- Establishing and maintaining a comprehensive, multi-tiered, dynamic information-sharing network designed to provide timely and actionable threat information, assessments, and warnings to public and private sector partners. This responsibility includes protecting sensitive information voluntarily provided by the private sector and facilitating the development of sector-specific and cross-sector information-sharing and analysis systems, mechanisms, and processes;
- Coordinating national efforts for the security of cyber infrastructure, including precursors and indicators of an attack, and understanding those threats in terms of CIKR vulnerabilities;
- Coordinating, facilitating, and supporting comprehensive risk assessment programs for high-risk CIKR, identifying priorities across sectors and jurisdictions, and integrating CIKR protection and resiliency programs with the all-hazards approach to domestic incident management described in HSPD-5;
- Facilitating the sharing of best practices and processes, and risk assessment methodologies and tools across sectors and jurisdictions;
- Ensuring that interagency, sector, and cross-sector coordination and information-sharing mechanisms and resources (e.g., DHS sector specialists) are in place to support CIKR-related incident management operations;
- Sponsoring CIKR protection-related R&D, demonstration projects, and pilot programs;
- Supporting the development and transfer of advanced technologies while leveraging private sector expertise and competencies, including participation in the development of voluntary standards or best practices, as appropriate;
- Promoting national-level CIKR protection education, training, and awareness in cooperation with State, local, tribal, territorial, regional, and private sector partners;
- Identifying and implementing plans and processes for appropriate increases in protective measures that align to all-hazards warnings; specific threats, as appropriate; and each level of the Homeland Security Advisory System (HSAS);
- Providing real-time (24/7) threat and incident reporting;
- Conducting modeling and simulations to analyze sector, cross-sector, and regional dependencies and interdependencies, to include cyber, and sharing the results with CIKR partners, as appropriate;
- Helping inform the annual Federal budget process based on CIKR risk and the potential for reducing risk and need, in coordination with SSAs, GCCs, and other partners;
- Supporting performance measurement for the national CIKR protection program and NIPP implementation process to encourage continuous improvement and providing annual CIKR protection reports to the Executive Office of the President (EOP) and Congress;
- Integrating national efforts for the protection and recovery of critical information systems and the cyber components of physical CIKR, including analysis, warning, information-sharing, and risk management activities and programs;
- Evaluating preparedness for CIKR protection across sectors and jurisdictions;
- Documenting lessons learned from exercises, actual incidents, and pre-disaster mitigation efforts and applying those lessons, where applicable, to CIKR protection efforts;
- Promoting CIKR awareness to provide incentives for participation by CIKR owners and operators;
- Working with the Department of State, SSAs, and other partners to ensure that U.S. CIKR protection efforts are fully coordinated with international partners; and
- Evaluating the need for and coordinating the protection of additional CIKR categories over time, as appropriate.

2.2.2 Sector-Specific Agencies

Recognizing that each CIKR sector possesses its own unique characteristics, operating models, and risk landscapes, HSPD-7 designates Federal Government SSAs for each of the CIKR sectors (see table 2-1). The SSAs are responsible for working with DHS and their respective GCCs to: implement the NIPP sector partnership model and risk management framework; develop protective programs, resiliency strategies, and related requirements; and provide sector-level CIKR protection guidance in line with the overarching guidance established by DHS pursuant to HSPD-7. Working in collaboration with partners, the SSAs are responsible for developing or revising and then submitting SSPs and sector-level performance feedback reports to DHS to enable national cross-sector CIKR protection program assessments.

In accordance with HSPD-7, SSAs are also responsible for collaborating with private sector partners and encouraging the development of appropriate voluntary information-sharing and analysis mechanisms within the sector. This includes encouraging voluntary security-related information sharing, where possible, among private entities within the sector, as well as among public and private entities.

Consistent with existing authorities (including regulatory authorities in some instances), SSAs perform the activities above, as appropriate, and in close cooperation with other sector partners. HSPD-7 requires SSAs to provide an annual report to the Secretary of Homeland Security on their efforts to identify, prioritize, and coordinate CIKR protection and resiliency in their respective sectors. DHS provides guidance and templates that inform reporting on sector CIKR protection priorities, requirements, and resources. The SSA's established annual budget process is the primary mechanism for outlining these sector-specific CIKR protection requirements and related budget projections, to the extent possible, as a component of their annual budget submissions to the Office of Management and Budget (OMB).

Additional SSA responsibilities include:

- Identifying, prioritizing, and coordinating Federal activities in support of CIKR protection and resiliency within the sector, with a particular focus on CIKR that could be exploited to cause catastrophic health effects or mass casualties comparable to those produced by a WMD;
- Managing the overall process for building partnerships and leveraging CIKR security expertise, relationships, and resources within the sector, including sector-level oversight and support of the sector partnership model described in chapter 4;
- Coordinating, facilitating, and supporting comprehensive risk assessment/management programs for high-risk CIKR, identifying protection and resiliency priorities, and incorporating CIKR protection activities as a key component of the all-hazards approach to domestic incident management within the sector;
- Facilitating the sharing of real-time incident notification, as well as CIKR protection best practices and processes, and risk assessment methodologies and tools within the sector;
- Promoting CIKR protection education, training, and awareness within the sector in coordination with State, regional, local, tribal, territorial, and private sector partners;
- Helping inform the annual Federal budget process considering CIKR risk and protection needs in coordination with partners and allocating resources for CIKR protection accordingly;
- Supporting performance measures for CIKR protection and NIPP implementation activities within the sector to enable continuous improvement, and reporting progress and gaps to DHS;
- Contributing to the annual National Critical Infrastructure Protection Research and Development (NCIP R&D) Plan;
- Identifying/recommending appropriate strategies to encourage private sector participation;
- Responding to or otherwise supporting DHS-initiated data calls, as appropriate, to populate the Infrastructure Data Warehouse (IDW), enable national-level risk assessment, and inform the national-level resource allocation;
- Supporting protocols for the Protected Critical Infrastructure Information (PCII) Program, as appropriate;
- Working with DHS, as appropriate, to develop and evaluate sector-specific risk assessment tools;
- Supporting dependency, interdependency, consequence, and other sector analyses, as needed;
- Coordinating with DHS and other NIPP partners to promote CIKR awareness to encourage participation by CIKR owners and operators;
- Coordinating sector-level participation in the National Exercise Program (NEP) (through the NEP Executive Steering Committee representatives), Homeland Security Exercise and Evaluation Program (HSEEP), and other sector-level activities;

Table 2-1: Sector-Specific Agencies and Assigned CIKR Sectors

Sector-Specific Agency	Critical Infrastructure and Key Resources Sector
Department of Agriculture ^a Department of Health and Human Services ^b	Agriculture and Food
Department of Defense ^c	Defense Industrial Base
Department of Energy	Energy ^d
Department of Health and Human Services	Healthcare and Public Health
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Water ^e
Department of Homeland Security <i>Office of Infrastructure Protection</i>	Chemical Commercial Facilities Critical Manufacturing Dams Emergency Services Nuclear Reactors, Materials, and Waste
<i>Office of Cybersecurity and Communications</i>	Information Technology Communications
<i>Transportation Security Administration</i>	Postal and Shipping
<i>Transportation Security Administration United States Coast Guard^f</i>	Transportation Systems ^g
<i>Immigration and Customs Enforcement, Federal Protective Service</i>	Government Facilities ^h

^a The Department of Agriculture is responsible for agriculture and food (meat, poultry, and egg products).

^b The Department of Health and Human Services is responsible for food other than meat, poultry, and egg products.

^c Nothing in this plan impairs or otherwise affects the authority of the Secretary of Defense over the Department of Defense (DoD), including the chain of command for military forces from the President as Commander in Chief, to the Secretary of Defense, to the commander of military forces, or military command and control procedures.

^d The Energy Sector includes the production, refining, storage, and distribution of oil, gas, and electric power, except for commercial nuclear power facilities.

^e The Water Sector includes drinking water and wastewater systems.

^f The U.S. Coast Guard is the SSA for the maritime transportation mode.

^g As stated in HSPD-7, the Department of Transportation and the Department of Homeland Security will collaborate on all matters relating to transportation security and transportation infrastructure protection.

^h The Department of Education is the SSA for the Education Facilities Subsector of the Government Facilities Sector.

- Assisting sector partners in their efforts to:
 - Organize and conduct protection and continuity-of-operations planning, and elevate awareness and understanding of threats and vulnerabilities to their assets, systems, and networks; and
 - Identify and promote effective sector-specific best practices and methodologies;
- Supporting the identification and implementation of plans and processes within the sector for enhancements in protective measures that align to all-hazards warnings; specific threats, as appropriate; and each level of the HSAS;
- Understanding and mitigating sector-specific cyber risk by developing or encouraging appropriate protective measures, information-sharing mechanisms, and emergency recovery plans for cyber assets, systems, and networks within the sector and interdependent sectors; and
- Coordinating with DHS, the Department of State (DOS), and other appropriate departments and agencies to integrate U.S. CIKR protection programs into the international and global markets, and address relevant dependency, interdependency, and cross-border issues.

2.2.3 Other Federal Departments, Agencies, and Offices

All Federal departments and agencies function as CIKR partners in coordination with DHS and the SSAs. In accordance with HSPD-7, they cooperate with DHS in implementing CIKR protection efforts, consistent with the Homeland Security Act and other applicable legal authorities. In this capacity, they support implementation of the NIPP and SSPs, as appropriate, and are responsible for supporting identification, prioritization, assessment, and remediation of, and enhancing the protection of, CIKR under their control. Federal departments and agencies that are not designated as SSAs, but that have unique responsibilities, functions, or expertise in a particular CIKR sector (such as GCC members) will:

- Assist in identifying and assessing high-consequence CIKR and enabling protective actions and programs within that sector;
- Support the national goal of enhancing CIKR protection through their role as the regulatory agency for owners and operators represented within a specific sector when so designated by statute; and
- Collaborate with all relevant partners to share security-related information within the sector, as appropriate.

Depending on their regulatory roles and their relationships with the SSAs, these agencies may play an important supporting role in developing and implementing the SSPs and related protective activities within the sector.

Under HSPD-7, a number of Federal departments and agencies and components of the EOP have special functions related to CIKR protection. The following section addresses Federal departments, agencies, and commissions specifically identified in HSPD-7. Many other Federal entities have sector-specific or cross-sector authorities and responsibilities that are more appropriately addressed in the SSPs.

- The DOS, in coordination with DHS and the Departments of Justice, Commerce, Defense, and the Treasury, works with foreign governments and international organizations to strengthen U.S. CIKR protection efforts.
- The Department of Justice (DOJ), including the Federal Bureau of Investigation (FBI), acts to reduce terrorist threats and investigates and prosecutes actual or attempted attacks on, sabotage of, or disruptions of CIKR in collaboration with DHS.
- The Department of Commerce (DOC) works with: DHS; the private sector; and research, academic, and government organizations to improve technology for cyber systems and promote other critical infrastructure efforts, including using its authority under the Defense Production Act to ensure the timely availability of materials, services, and facilities to meet homeland security requirements, and to address economic security issues.
- The Department of Transportation (DOT) collaborates with DHS on all matters related to transportation security and transportation infrastructure protection, and is also responsible for operating the National Airspace System. DOT and DHS collaborate on regulating the transportation of hazardous materials by all modes (including pipelines).
- The Nuclear Regulatory Commission (NRC) works with DHS and the Department of Energy (DOE), as appropriate, to ensure the protection of commercial nuclear reactors for generating electric power and non-power nuclear reactors used for research, testing, and training; nuclear materials in medical, industrial, and academic settings and facilities that fabricate nuclear fuel; and the transportation, storage, and disposal of commercial nuclear materials and waste. In addition, the NRC collaborates with DHS on any changes in the protective measures for this sector, as well as the approval of new reactor applications.

- The Intelligence Community, the Department of Defense (DoD), and other appropriate Federal departments, such as the Department of the Interior (DOI) and DOT, have collaborated with DHS to develop and implement a suite of geospatial visualization and analysis tools to map, image, analyze, and sort CIKR data using commercial satellite and airborne systems, as well as associated agency capabilities. DHS works with these Federal departments and agencies to identify and help protect those positioning, navigation, and timing services, such as global positioning systems (GPS), that are critical enablers for CIKR sectors such as Banking and Finance and Communications. DHS and the Intelligence Community also collaborate with other agencies, such as the Environmental Protection Agency, that manage data addressed by geographic information systems.
- The Homeland Security Council ensures the coordination of interagency policy related to physical and cyber CIKR protection based on advice from the Critical Infrastructure Protection Policy Coordination Committee (PCC). This PCC is chaired by a Federal officer or employee designated by the Assistant to the President for Homeland Security.
- The White House Office of Science and Technology Policy coordinates with DHS to further interagency R&D related to CIKR protection.
- The OMB oversees the implementation of government-wide policies, principles, standards, and guidelines for Federal Government computer security programs.

2.2.4 State, Local, Tribal, and Territorial Governments

State, local, tribal, and territorial governments are responsible for implementing the homeland security mission, protecting public safety and welfare, and ensuring the provision of essential services to communities and industries within their jurisdictions. They also play a very important and direct role in enabling CIKR protection and resiliency, including CIKR under their control, as well as that owned and operated by other NIPP partners within their jurisdictions. The efforts of these public entities are critical to the effective implementation of the NIPP, SSPs, and various jurisdictionally focused protection and resiliency plans. They are equally critical in terms of enabling time-sensitive, post-event CIKR response and recovery activities.

CIKR partners at all levels of government have developed homeland security strategies that align with and support the priorities established in the National Preparedness Guidelines. With the inclusion of NIPP implementation as one of these national priorities, CIKR protection programs form an

essential component of State, local, tribal, and territorial homeland security strategies, particularly with regard to establishing funding priorities and informing security investment decisions. To permit effective NIPP implementation and performance measurement at each jurisdictional level, these protection programs should reference all core elements of the NIPP framework, where appropriate, including key cross-jurisdictional security and information-sharing linkages, as well as specific CIKR protection programs focused on risk management. These programs play a primary role in the identification and protection of CIKR regionally and locally and also support DHS and SSA efforts to identify, ensure connectivity with, and enable the protection of CIKR of national-level criticality within the jurisdiction.

2.2.4.1 State and Territorial Governments

State (and territorial, where applicable) governments are responsible for establishing partnerships, facilitating coordinated information sharing, and enabling planning and preparedness for CIKR protection within their jurisdictions. They serve as crucial coordination hubs, bringing together prevention, protection, response, and recovery authorities; capabilities; and resources among local jurisdictions, across sectors, and between regional entities. States and territories also act as conduits for requests for Federal assistance when the threat or incident situation exceeds the capabilities of public and private sector partners at lower jurisdictional levels. States receive CIKR information from the Federal Government to support national and State CIKR protection and resiliency programs.

State and territorial governments shall develop and implement State or territory-wide CIKR protection programs that reflect the full range of NIPP-related activities. State and territorial programs should address all relevant aspects of CIKR protection, leverage support from homeland security assistance programs that apply across the homeland security mission area, and reflect priority activities in their strategies to ensure that resources are effectively allocated. Effective statewide and regional CIKR protection efforts should be integrated into the overarching homeland security program framework at the State or territory level to ensure that prevention, protection, response, and recovery efforts are synchronized and mutually supportive. CIKR protection at the State or territory level must cut across all sectors present within the State or territory and support national, State, and local priorities. The program also should explicitly address unique geographical issues, including transborder concerns, as well as interdependencies among sectors and jurisdictions within those geographical boundaries.

Specific CIKR protection-related activities at the State and territorial level include, but are not limited to:

- Acting as a focal point for and promoting the coordination of protective and emergency response activities, preparedness programs, and resource support among local jurisdictions, regional organizations, and private sector partners;
- Developing a consistent approach to CIKR identification, risk determination, mitigation planning, and prioritized security investment, and exercising preparedness among all relevant stakeholders within their jurisdictions;
- Identifying, implementing, and monitoring a risk management plan and taking corrective actions, as appropriate;
- Participating in significant national, regional, and local awareness programs to encourage appropriate management and security of cyber systems;
- Acting as conduits for requests for Federal assistance when the threat or current situation exceeds the capabilities of State and local jurisdictions and the private entities resident within them;
- Facilitating the exchange of security information, including threat assessments and other analyses, attack indications and warnings, and advisories, within and across jurisdictions and sectors therein;
- Participating in the NIPP sector partnership model, including: sector-specific GCCs; the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC); SCCs; and other CIKR governance and planning efforts relevant to the given jurisdiction;
- Ensuring that funding priorities are addressed and that resources are allocated efficiently and effectively to achieve the CIKR protection mission in accordance with relevant plans and strategies;
- Sharing information on CIKR deemed to be critical from national, State, regional, local, tribal, and/or territorial perspectives to enable prioritized protection and restoration of critical public services, facilities, utilities, and functions within the jurisdiction;
- Addressing unique geographical issues, including transborder concerns, dependencies, and interdependencies among the sectors within the jurisdiction;
- Identifying and implementing plans and processes for increasing protective measures that align to all-hazards warnings; specific threats, as appropriate; and each level of the HSAS;

- Documenting lessons learned from pre-disaster mitigation efforts, exercises, and actual incidents, and applying that learning, where applicable, to the CIKR context;
- Coordinating with NIPP partners to promote CIKR awareness to motivate participation by CIKR owners and operators;
- Providing response and protection, as appropriate, where there are gaps and where local entities lack the resources needed to address those gaps;
- Identifying and communicating the requirements for CIKR-related R&D to DHS; and
- Providing information, as part of the grants process and/or homeland security strategy updates, regarding State priorities, requirements, and CIKR-related funding needs.

2.2.4.2 Regional Organizations

Regional partnerships include a variety of public-private sector initiatives that cross jurisdictional and/or sector boundaries and focus on homeland security preparedness, protection, response, and recovery within or serving the population of a defined geographical area. Specific regional initiatives range in scope from organizations that include multiple jurisdictions and industry partners within a single State to groups that involve jurisdictions and enterprises in more than one State and across international borders. In many cases, State governments also collaborate through the adoption of interstate compacts to formalize regionally based partnerships regarding CIKR protection.

Partners leading or participating in regional initiatives are encouraged to capitalize on the larger area- and sector-specific expertise and relationships to:

- Promote collaboration among partners in implementing NIPP-related CIKR risk assessment and protection activities;
- Facilitate education and awareness of CIKR protection efforts occurring within their geographical areas;
- Participate in regional exercise and training programs, including a focus on CIKR protection collaboration across jurisdictional and sector boundaries;
- Support threat-initiated and ongoing operations-based activities to enhance protection and preparedness, as well as to support mitigation, response, and recovery;
- Work with State, local, tribal, territorial, and international governments and the private sector, as appropriate, to evaluate regional and cross-sector CIKR interdependencies, including cyber considerations;

- Conduct the appropriate regional planning efforts and undertake appropriate partnership agreements to enable regional CIKR protection activities and enhanced response to emergencies;
- Facilitate information sharing and data collection between and among regional initiative members and external partners;
- Share information on progress and CIKR protection requirements with DHS, the SSAs, State and local governments, and other CIKR partners, as appropriate; and
- Participate in the NIPP sector partnership model, as appropriate.

2.2.4.3 Local Governments

Local governments represent the front lines for homeland security and, more specifically, CIKR protection and implementation of the NIPP partnership model. They provide critical public services and functions in conjunction with private sector owners and operators. In some sectors, local governmental entities own and operate CIKR such as water, stormwater, and electric utilities. Most disruptions or malevolent acts that affect CIKR begin and end as local situations. Local authorities typically shoulder the weight of initial prevention, response, and recovery operations until coordinated support from other sources becomes available, regardless of who owns or operates the affected asset, system, or network. As a result, local governments are critical partners under the NIPP framework. They drive emergency preparedness, as well as local participation in NIPP and SSP implementation across a variety of jurisdictional partners, including government agencies, owners and operators, and private citizens in the communities that they serve.

CIKR protection focus at the local level should include, but is not limited to:

- Acting as a focal point for and promoting the coordination of protective and emergency response activities, preparedness programs, and resource support among local agencies, businesses, and citizens;
- Developing a consistent approach at the local level to CIKR identification, risk determination, mitigation planning, and prioritized security investment, and exercising preparedness among all relevant partners within the jurisdiction;
- Identifying, implementing, and monitoring a risk management plan, and taking corrective actions, as appropriate;
- Participating in significant national, State, local, and regional education and awareness programs to encourage appropriate management and security of cyber systems;

- Facilitating the exchange of security information, including threat assessments, attack indications and warnings, and advisories, among partners within the jurisdiction;
- Participating in the NIPP sector partnership model, including GCCs, SCCs, SLTTGCC, and other CIKR structures relevant to the given jurisdiction;
- Ensuring that funding priorities are addressed and that resources are allocated efficiently and effectively to achieve the CIKR protection mission in accordance with relevant plans and strategies;
- Establishing continuity plans and programs that facilitate the performance of critical functions during an emergency or until normal operations can be resumed;
- Sharing with partners, as appropriate, CIKR information deemed to be critical from the local perspective to enable prioritized protection and restoration of critical public services, facilities, utilities, and processes within the jurisdiction;
- Addressing unique geographical issues, including transborder concerns, dependencies, and interdependencies among agencies and enterprises within the jurisdiction;
- Identifying and implementing plans and processes for steps in protective measures that align to all-hazards warnings; specific threats, as appropriate; and each level of the HSAS;
- Documenting lessons learned from pre-disaster mitigation efforts, exercises, and actual incidents, and applying that learning, where applicable, to the CIKR protection context; and
- Conducting CIKR protection public awareness activities.

2.2.4.4 Tribal Governments

Tribal government roles and responsibilities regarding CIKR protection generally mirror those of State and local governments as detailed above. Tribal governments are accountable for the public health, welfare, and safety of tribal members, as well as the protection of CIKR and the continuity of essential services under their jurisdiction. Under the NIPP partnership model, tribal governments shall ensure coordination with Federal, State, local, and international counterparts to achieve synergy in the implementation of the NIPP and SSP frameworks within their jurisdictions. This is particularly important in the context of information sharing, risk analysis and management, awareness, preparedness planning, and protective program investments and initiatives.

2.2.4.5 Boards, Commissions, Authorities, Councils, and Other Entities

An array of boards, commissions, authorities, councils, and other entities at the State, local, tribal, and regional levels perform regulatory, advisory, policy, or business oversight functions related to various aspects of CIKR operations and protection within and across sectors and jurisdictions. Some of these entities are established through State- or local-level executive or legislative mandates with elected, appointed, or voluntary membership. These groups include, but are not limited to, transportation authorities, public utility commissions, water and sewer boards, park commissions, housing authorities, public health agencies, and many others. These entities may serve as the equivalents of SSAs within a State and contribute expertise, assist with regulatory authorities, or help facilitate investment decisions related to CIKR protection efforts within a given jurisdiction or geographical region.

2.2.5 CIKR Owners and Operators

Owners and operators generally develop and implement the protective programs and resiliency strategies for the CIKR under their control. CIKR are owned by both the public and private sector; however, the majority of CIKR is owned by the private sector. Owners and operators take action to support risk management planning and investments in security as a necessary component of prudent business planning and operations. In today's risk environment, these activities generally include reassessing and adjusting continuity-of-business and emergency management plans, building increased resiliency and redundancy into business processes and systems, protecting facilities against physical and cyber attacks, reducing the vulnerability to natural disasters, guarding against insider threats, and increasing coordination with external organizations to avoid or minimize the impact on surrounding communities or other industry partners.

For many private sector enterprises, the level of investment in security reflects risk-versus-consequence tradeoffs that are based on two factors: (1) what is known about the risk environment, and (2) what is economically justifiable and sustainable in a competitive marketplace or within resource constraints. In the context of the first factor, the Federal Government is uniquely positioned to help inform critical security investment decisions and operational planning. For example, owners and operators generally look to the government as a source of security-related best practices and for attack or natural hazard indications, warnings, and threat assessments. In relation to the second factor, owners and operators also generally rely on governmental entities

to address risks outside of their property or in situations in which the current threat exceeds an enterprise's capability to protect itself or requires an unreasonable level of additional investment to mitigate risk. In this situation, public and private sector partners at all levels must collaborate to address the protection of national-level CIKR, provide timely warnings, and promote an environment in which CIKR owners and operators can better carry out their specific protection responsibilities. Additionally, CIKR owners and operators may be required to invest in security as a result of Federal, State, and/or local regulations.

The CIKR protection responsibilities of specific owners or operators vary widely within and across sectors. Some sectors have regulatory or statutory frameworks that govern private sector security operations within the sector; however, most are guided by voluntary security regimes or adherence to industry-promoted best practices. Within this diverse protective landscape, private sector entities can better secure the CIKR under their control by:

- Performing comprehensive risk assessments tailored to their specific sector, enterprise, or facility risk landscape;
- Implementing protective actions and programs to reduce identified vulnerabilities appropriate to the level of risk presented;
- Participating in the NIPP sector partnership model (including SCCs and information-sharing mechanisms);
- Developing an awareness of critical dependencies and interdependencies at the sector, enterprise, and facility levels;
- Assisting and supporting Federal, State, local, and tribal government CIKR data collection and protection efforts;
- Developing and coordinating CIKR protective and emergency response actions, plans, and programs with appropriate Federal, State, and local government authorities;
- Establishing continuity plans and programs that facilitate the performance of critical functions during an emergency or until normal operations can be resumed;
- Establishing cybersecurity programs and associated awareness training within the organization;
- Adhering to recognized industry best business practices and standards, including those with a cybersecurity nexus (see appendix 5B);
- Participating in Federal, State, local, and tribal government emergency management programs and coordinating structures;

- Establishing resilient, robust, and/or redundant operational systems or capabilities associated with critical functions;
- Promoting CIKR protection education, training, and awareness programs;
- Adopting and implementing effective workforce security assurance programs to mitigate potential insider threats;
- Providing technical expertise to the SSAs and DHS;
- Participating in regular CIKR protection-focused training and exercise programs with other public and private sector partners;
- Identifying and communicating requirements to DHS and/or the SSAs and State and local governments for CIKR protection-related R&D;
- Sharing security-related best practices and entering into operational mutual-aid agreements with other industry partners; and
- Working to identify and reduce barriers to public-private partnerships.

2.2.6 Advisory Councils

Advisory councils provide advice, recommendations, and expertise to the government (e.g., DHS, SSAs, and State or local agencies) regarding CIKR protection policy and activities. These entities also help enhance public-private partnerships and information sharing. They often provide an additional mechanism to engage with a pre-existing group of private sector leaders to obtain feedback on CIKR protection policy and programs, and to make suggestions to increase the efficiency and effectiveness of specific government programs. Examples of CIKR protection-related advisory councils and their associated responsibilities include:

- **Critical Infrastructure Partnership Advisory Council (CIPAC):** CIPAC is a partnership between government and private sector CIKR owners and operators that facilitates effective coordination of Federal CIKR protection programs. CIPAC engages in a range of CIKR protection activities, such as planning, risk assessments, coordination, NIPP implementation, and operational activities, including incident response and recovery. DHS published a Federal Register Notice on March 24, 2006, announcing the establishment of CIPAC as a Federal Advisory Committee Act (FACA)⁵-exempt body pursuant to section 871 of the Homeland Security Act (see chapter 4).

- **Homeland Security Advisory Council (HSAC):** HSAC provides advice and recommendations to the Secretary of Homeland Security on relevant issues. The Council members, appointed by the DHS Secretary, include experts from State and local governments, public safety, security and first-responder communities, academia, and the private sector.
 - Private Sector Senior Advisory Committee (PVSAC): The Secretary of Homeland Security established PVSAC as a subcommittee of HSAC in order to provide HSAC with expert advice from leaders in the private sector.
- **National Infrastructure Advisory Council (NIAC):** NIAC provides the President, through the Secretary of Homeland Security, with advice on the security of physical and cyber systems across all CIKR sectors. The council comprises up to 30 members appointed by the President. Members are selected from the private sector, academia, and State and local governments. The council was established (and amended) under Executive Orders 13231, 13286, and 13385.
- **National Security Telecommunications Advisory Committee (NSTAC):** NSTAC provides industry-based advice and expertise to the President on issues and problems related to implementing National Security and Emergency Preparedness (NS/EP) communications policy. NSTAC, created under Executive Order 12382, comprises up to 30 industry chief executives representing the major communications and network service providers and information technology, finance, and aerospace companies.

2.2.7 Academia and Research Centers

The academic and research center communities play an important role in enabling national-level CIKR protection and implementation of the NIPP, including:

- Establishing Centers of Excellence (i.e., university-based partnerships or federally funded R&D centers) to provide independent analysis of CIKR protection issues;
- Supporting the research, development, testing, evaluation, and deployment of CIKR protection technologies;
- Analyzing, developing, and sharing best practices related to CIKR prioritization and protection efforts;
- Researching and providing innovative thinking and perspective on threats and the behavioral aspects of terrorism;

⁵ FACA authorized the establishment of a system governing the creation and operation of advisory committees in the executive branch of the Federal Government and for other purposes. The act, when it applies, generally requires advisory committees to meet in open session and make publicly available associated written materials. It also requires a 15-day notice before any meeting may be closed to public attendance, a requirement that could prevent a meeting on short notice to discuss sensitive information in an appropriate setting.

- Preparing or disseminating guidelines, courses, and descriptions of best practices for physical security and cybersecurity;
- Developing and providing suitable all-hazards risk analysis and risk management courses for CIKR protection professionals;
- Establishing undergraduate and graduate curricula and degree programs;
- Conducting research to identify new technologies and analytical methods that can be applied by partners to support NIPP efforts; and
- Participating in the review and validation of NIPP-supporting risk analysis and management approaches.

3. The Strategy: Managing Risk

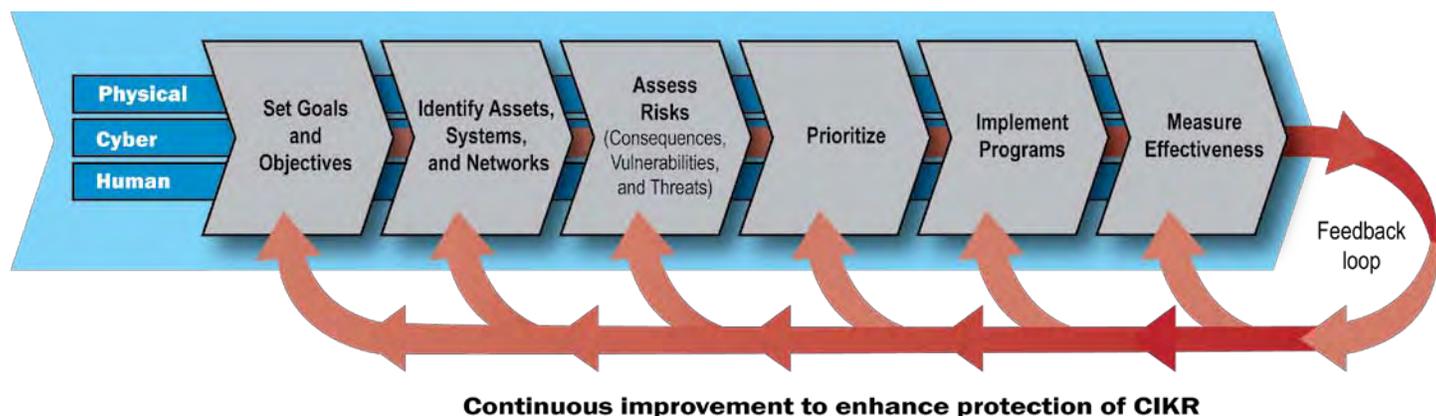
The cornerstone of the NIPP is its risk management framework. Risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. Simply stated, risk is influenced by the nature and magnitude of a threat, the vulnerabilities to that threat, and the consequences that could result. Risk is an important means of prioritizing mitigation efforts for partners ranging from facility owners and operators to Federal agencies. The NIPP risk management framework (see figure 3-1) integrates and coordinates strategies, capabilities, and governance to enable risk-informed decisionmaking related to the Nation’s CIKR. This framework is applicable to threats such as natural disasters, manmade safety hazards, and terrorism, although different information and methodologies may be used to understand each.

This chapter addresses the use of the NIPP risk management framework as part of the overall effort to ensure the protection and resiliency of our Nation’s CIKR. DHS, the SSAs, and their public and private sector partners share responsibility for implementation of the NIPP risk management framework. The SSAs are responsible for leading sector-specific risk management programs and for ensuring that the tailored, sector-specific application of the risk management framework is addressed in their respective SSPs. DHS supports these efforts by providing guidance and analytical support to the SSAs and other partners. DHS, in collaboration with other CIKR partners, is responsible for using the best avail-

able information to conduct cross-sector risk analysis and risk management activities. This includes the assessment of: dependencies, interdependencies, and cascading effects; identification of common vulnerabilities; development and sharing of common threat scenarios; assessment and comparison of risk across sectors; identification and prioritization of risk management opportunities across sectors; development and sharing of cross-sector measures to reduce or manage risk; and identification of specific cross-sector R&D needs.

The NIPP risk management framework is tailored toward and applied on an asset, system, network, or functional basis,

Figure 3-1: NIPP Risk Management Framework



depending on the fundamental characteristics of the individual CIKR sectors. For those sectors primarily dependent on fixed assets and physical facilities, a bottom-up, asset-by-asset approach may be most appropriate. For sectors such as Communications, Information Technology, and Agriculture and Food, with accessible and distributed systems, a top-down, business or mission continuity approach, or risk assessments that focus on network and system interdependencies may be more effective. Each sector must pursue the approach that produces the most effective use of resources for the sector and contributes to cross-sector comparative risk analyses conducted by DHS.

The NIPP risk management framework includes the following activities:

- **Set goals and objectives:** Define specific outcomes, conditions, end points, or performance targets that collectively constitute an effective risk management posture.
- **Identify assets, systems, and networks:** Develop an inventory of the assets, systems, and networks, including those located outside the United States, that make up the Nation's CIKR or contribute to the critical functionality therein, and collect information pertinent to risk management that takes into account the fundamental characteristics of each sector.
- **Assess risks:** Evaluate the risk, taking into consideration the potential direct and indirect consequences of a terrorist attack or other hazards (including, as capabilities mature, seasonal changes in the consequences and dependencies and interdependencies associated with each identified asset, system, or network), known vulnerabilities to various potential attack methods or other significant hazards, and general or specific threat information.
- **Prioritize:** Aggregate and compare risk assessment results to: develop an appropriate view of asset, system, and/or network risks and associated mission continuity, where applicable; establish priorities based on risk; and determine protection, resilience, or business continuity initiatives that provide the greatest return on investment for the mitigation of risk.
- **Implement protective programs and resiliency strategies:** Select appropriate actions or programs to reduce or manage the risk identified; identify and provide the resources needed to address priorities.
- **Measure effectiveness:** Use metrics and other evaluation procedures at the appropriate national, State, local, regional, and sector levels to measure progress and assess the effectiveness of the CIKR protection programs.

This process features a continuous feedback loop, which allows the Federal Government and its CIKR partners to track progress and implement actions to improve national CIKR protection and resiliency over time. The physical, cyber, and human elements of CIKR should be considered in tandem in each aspect of the risk management framework. The sector partnership model discussed in chapter 4 provides the structure for coordination and management of risk management activities that are flexibly tailored to different sectors and levels of government.

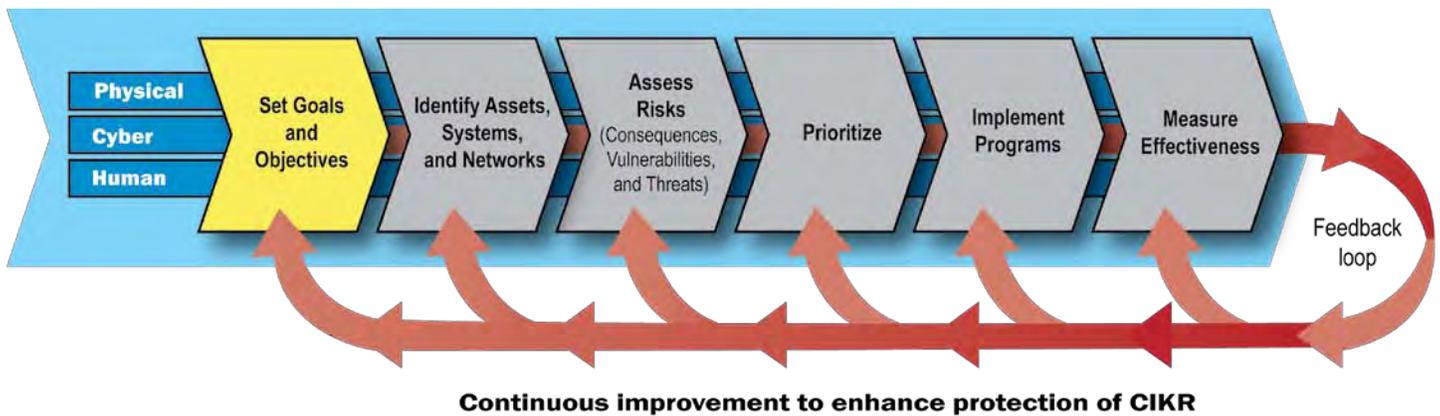
3.1 Set Goals and Objectives

Achieving robust, protected, and resilient infrastructure requires national, State, local, and sector-specific CIKR protection visions, goals, and objectives that describe the desired risk management posture. These goals and objectives should consider the physical, cyber, and human elements of CIKR protection and resiliency. Goals and objectives may vary across and within sectors and levels of government, depending on the risk landscape, operating environment, and composition of a specific industry, resource, or other aspect of CIKR.

Nationally, the overall goal of CIKR-related risk management is an enhanced state of protection and resilience achieved through the implementation of focused risk-reduction strategies within and across sectors and levels of government. The NIPP risk management framework supports this goal by:

- Enabling the development of the national, State, regional, and sector risk profiles that serve as the foundation for the National CIKR Protection Annual Report described in chapter 7. These risk profiles outline the highest risks facing different sectors and geographical regions, and identify cross-sector or regional issues of concern that are appropriate for the Federal CIKR protection focus, as well as opportunities for sector-, State-, and regionally based initiatives.
- Enabling DHS, SSAs, and other partners to determine the best courses of action to reduce potential consequences, threats, or vulnerabilities. Some available options include encouraging voluntary implementation of focused risk management strategies (e.g., through public-private partnerships), pursuing economic incentive-related policies and programs, and undertaking regulatory action, if appropriate; and
- Allowing the identification of risk management and resource allocation options for CIKR owners and operators, as well as different government partners.

Figure 3-2: NIPP Risk Management Framework: Set Goals and Objectives



From a sector or jurisdictional perspective, CIKR protection goals or their related supporting objectives:

- Consider distinct assets, systems, networks, functions, operational processes, business environments, and risk management approaches;
- Define the risk management posture that CIKR partners seek to attain; and
- Express this posture in terms of the outcomes and objectives sought.

Taken collectively, these goals and objectives guide all levels of government and the private sector in tailoring risk management programs and activities to address CIKR protection and resilience needs.

3.2 Identify Assets, Systems, and Networks

To meet its responsibilities under the Homeland Security Act and HSPD-7, DHS continuously engages partner agencies and other CIKR partners to build, manage, refine, and improve a comprehensive inventory of the assets, systems, and networks that make up the Nation’s CIKR. This inventory provides a common baseline of knowledge that can support CIKR partners at various levels of government and the private sector in understanding infrastructure dependencies and interdependencies, as well as enable national, local, regional, and sector-based risk assessment, prioritization, and management.

Given the Nation’s vast and varied infrastructure, developing an inventory of critical assets, systems, and networks will vary by sector and types of CIKR.

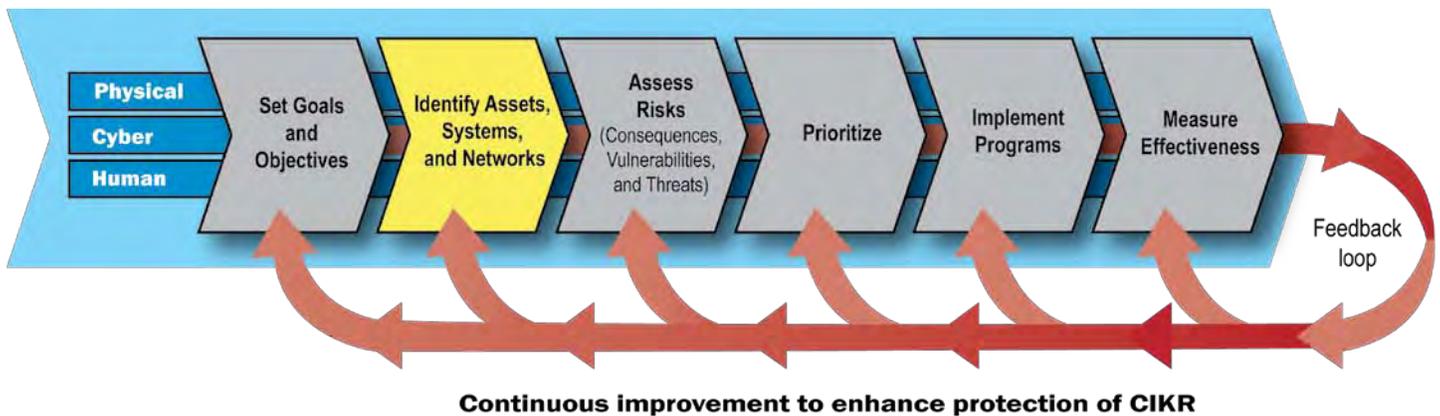
3.2.1 National Infrastructure Inventory

DHS maintains a national inventory of the assets, systems, and networks that make up the Nation’s CIKR. The Nation’s infrastructure includes assets, systems, and networks that are nationally significant and those that may not be significant on a national level but are, nonetheless, important to State, local, or regional CIKR protection, incident management, and response and recovery efforts. The principal national inventory of CIKR systems and assets is the IDW. The IDW comprises a federated data architecture that provides a single virtual view of one or more infrastructure data sources. DHS uses this data to provide all relevant public and private sector CIKR partners with access to the most current and complete view of the Nation’s infrastructure information allowed under applicable Federal, State, or local regulation. Section 3.2.2 discusses protecting and accessing this data.

The goal of the IDW is to provide access to relevant information for natural disasters, industrial accidents, and other incidents, as well as maintain basic information about the relationships, dependencies, and interdependencies among various assets, systems, and networks, including foreign CIKR on which the United States may rely. The inventory will also eventually include a cyber data framework to characterize each sector’s unique and significant cyber assets, systems, or networks.

This information is needed not only to help manage CIKR protection and resiliency approaches, but also to inform and support the response to a wide array of incidents and emergencies. Risk may change based on many factors including damage resulting from a natural disaster; seasonal or cyclic dependencies; and changes in technology, the economy, or the terrorist threat. The inventory supports domestic incident

Figure 3-3: NIPP Risk Management Framework: Identify Assets, Systems, and Networks



management by helping to: prioritize and focus preparedness planning; inform decisionmaking; establish strategies for response; and identify priorities for restoration, remediation, and reconstruction.

Currently, the inventory and associated attributes are maintained through the Infrastructure Information Collection System (IICS), a federated IDW, accessible in a geospatial context using the capabilities provided by the Integrated Common Analytical Viewer (iCAV) suite of tools, including the iCAV and DHS Earth viewers. The SSAs and DHS work together and in concert with State, local, tribal, and territorial governments and private sector partners to ensure that the inventory data structure is accurate, current, and secure. DHS provides guidelines concerning information needed to develop and maintain the inventory. Within this inventory, the set of nationally and regionally significant infrastructure is maintained and constantly updated and refined.

Information in the IDW comes from a variety of sources and takes advantage of work that has already been done, such as:

- **Sector inventories:** SSAs and GCCs maintain close working relationships with owners and operators, SCCs, and other sources that maintain the inventories necessary for the sector’s business or mission. CIKR partners provide relevant information to DHS and update it on a periodic basis to ensure that sector CIKR and associated critical functionality are adequately represented and that sector and cross-sector dependencies and interdependencies can be identified and analyzed.
- **Voluntary submissions from CIKR partners:** Owners and operators; State, local, tribal, and territorial governments; and Federal departments and agencies voluntarily submit information and previously completed inventories and analyses for DHS to consider.

- **Results of studies:** Various government or commercial databases developed as a result of studies undertaken by trade associations, advocacy groups, and regulatory agencies may contain relevant information.
- **Annual data calls:** DHS, in cooperation with the SSAs and other CIKR partners, conducts a voluntary annual data call to State, territorial, and Federal partners. This data call process allows State, territorial, and Federal partners to propose CIKR data inputs meeting specified criteria.
- **Ongoing reviews of particular locations where risk is believed to be higher:** DHS- and SSA-initiated site assessments to: provide information on vulnerability; help identify assets, systems, and networks and their dependencies, interdependencies, and critical functionality; and provide information that will help quantify their value in risk analyses.

DHS, in coordination with the SSAs, State and local governments, private sector owners and operators, and other partners, works to build from and update existing inventories at the State and local levels to avoid duplication of past or ongoing complementary efforts.

3.2.2 Protecting and Accessing Inventory Information

The Federal Government recognizes the sensitive, business, or proprietary nature of much of the information accessed through the IDW. DHS is responsible for protecting this information from unauthorized disclosure or use. Information in the IDW is protected from unauthorized disclosure or misuse to the maximum extent allowed under applicable Federal, State, or local regulations, including PCII and security classification rules (see section 4.3). Additionally, DHS ensures that all data and licensing restrictions are strictly enforced. DHS is implementing important resilient

and redundant security measures that apply to the IDW and provide system integrity and security, software security, and data protection.

3.2.3 SSA Role in Inventory Development and Maintenance

The SSAs have a leading role in several phases of CIKR inventory development and maintenance, including nominating assets and systems and adjudication of those high-risk assets and systems proposed by States and territories in response to the annual data call.

The specific methods by which the SSAs collect sector-specific asset, system, and network data vary by sector and are described in the individual SSPs. The SSPs include descriptions of mechanisms for making data collection efforts more manageable and less burdensome, such as:

- Prioritizing the approach for data outreach to different partners;
- Identifying assets, systems, networks, or functions of potential national-, regional-, or sector-level importance; and
- Identifying, reviewing, and leveraging existing sector infrastructure data sources.

The SSAs enable sector-specific asset, system, and network awareness, data collection, and information sharing primarily by understanding existing sector-based data sources and by facilitating information-sharing agreements with data owners. For example, DHS, in its capacity as the SSA for the Dams Sector (which includes locks and levees), works closely with the U.S. Army Corps of Engineers (USACE) in the Dams Sector to facilitate data discovery within the National Inventory of Dams (NID). Although owned and maintained by USACE, shared access to the NID provides CIKR partners in Federal, State, and local governments and the private sector with a comprehensive understanding of the national dams landscape.

More details on SSA roles and responsibilities in facilitating sector awareness and understanding related to the IDW are included in appendix 3C.

3.2.4 State and Local Government Role in Inventory Development and Maintenance

State and local government agencies play an important role in understanding the national CIKR landscape by enabling the identification of assets, systems, and networks at the State and local levels. State and local first-responders, emergency

managers, public health officials, and others involved in homeland security missions frequently interact with infrastructure owners and operators in their jurisdictions to plan for and respond to all manner of natural and manmade hazards. These relationships form the core of the public-private partnership model and translate into first-hand knowledge of the infrastructure landscape at the State and local levels, as well as an understanding of those CIKR that are considered critical from a State and local perspective.

DHS provides a number of tools and resources to help State and local officials leverage their knowledge to create infrastructure inventories that contribute to the IDW. This includes the Constellation/Automated Critical Asset Management System (C/ACAMS) that helps State and local officials leverage their knowledge to create infrastructure inventories, implement practical CIKR protection programs, and facilitate information sharing within and across State and local boundaries, as well as with DHS and other Federal partners. By sharing first-hand knowledge and understanding through tools such as C/ACAMS, State and local partners contribute directly to the national CIKR protection mission.

Additional information on State roles and responsibilities in this area is contained in appendix 3C.

Constellation/Automated Critical Asset Management System

C/ACAMS is a Web-enabled information services portal that helps State and local governments build CIKR protection programs in their local jurisdictions. Specifically, C/ACAMS provides a set of tools and resources that help law enforcement, public safety, and emergency response personnel to:

- **Collect and use CIKR asset data;**
- **Assess CIKR asset vulnerabilities;**
- **Develop all-hazards incident response and recovery plans; and**
- **Build public-private partnerships.**

The Constellation portion of C/ACAMS is an information gathering and analysis tool that allows users to search a range of free and subscription reporting sources to find relevant information tailored to their jurisdiction's needs. ACAMS is a secure, online database and database management platform that allows for: the collection and management of CIKR asset data; the cataloging, screening, and sorting of this data; the production of tailored infrastructure reports; and the development of a variety of pre- and post-incident response plans that are useful for strategic and operational planners and tactical commanders. Email ACAMS-info@hq.dhs.gov for additional information.

3.2.5 Identifying Cyber Infrastructure

The NIPP addresses the protection of the cyber elements of CIKR in an integrated manner rather than as a separate consideration. As a component of the sector-specific risk assessment process, cyber infrastructure components should be identified individually or included as a cyber element of a larger asset, system, or network's description if they are associated with one. The identification process should include information on international cyber infrastructure with cross-border implications, interdependencies, or cross-sector ramifications. Cyber infrastructure that exist in most, if not all, sectors include business systems, control systems, access control systems, and warning and alert systems.

The Internet has been identified as a key resource, comprising the domestic and international assets within both the Information Technology and Communications Sectors, and is used by all sectors to varying degrees. While the availability of the service is the responsibility of both the Information Technology and Communications sectors, the need for access to and reliance on the Internet is common to all sectors.

DHS supports the SSAs and other CIKR partners by developing tools and methodologies to assist in identifying cyber assets, systems, and networks, including those that involve multiple sectors. As needed, DHS works with sector representatives to help identify cyber infrastructure within the NIPP risk management framework.

Additionally, DHS, in collaboration with other CIKR partners, provides cross-sector cyber methodologies that, when applied, enable sectors to identify cyber assets, systems, and networks that may have nationally significant consequences if destroyed, incapacitated, or exploited. These methodologies also characterize the reliance of a sector's business and operational functionality on cyber infrastructure components. Also, if an appropriate cyber identification methodology is already being used within the sector, DHS will work with the sector to ensure alignment of that methodology with the NIPP risk management framework.

3.2.6 Identifying Positioning, Navigation, and Timing Services

Space-based and terrestrial positioning, navigation, and timing (PNT) services are a component of multiple CIKR sectors. These services underpin almost every aspect of transportation across all its various modes. Additionally, the Banking and Finance, Communications, Energy, and Water Sectors rely on GPS as their primary timing source. The systems that support or enable critical functions in the CIKR sectors

should be identified, either as part of or independent of the infrastructure, as appropriate. Examples of CIKR functions that depend on PNT services include: aviation (navigation, air traffic control, surface guidance); maritime (harbor, inland waterway vessel movement, and maritime surveillance, such as Automatic Identification Systems (AIS)); surface transportation (rail, hazardous materials (HAZMAT) tracking); communications networks (global fiber and wireless networks); and power grids. PNT services must be reliable, seamless, resistant, and resilient to unintentional or intentional interference or jamming.

DHS has developed a PNT Interference Detection and Mitigation (IDM) Plan as required by the U.S. Space-Based PNT Policy of December 8, 2004. The policy established responsibilities for multiple departments and agencies within the Federal Government to better plan, manage, and protect PNT services, and assigned to the DHS specific responsibilities governing the protection of PNT services within CIKR. The IDM Plan details the DHS initial response to the policy implementation action and lays the foundation for further planning and actions necessary to meet the responsibilities. The IDM Plan was approved by the President on August 20, 2007.

3.3 Assess Risks

Common definitions, scenarios, assumptions, metrics, and processes are needed to ensure that risk assessments contribute to a shared understanding among CIKR partners. The approach outlined by the NIPP risk management framework results in sound, scenario-based consequence and vulnerability estimates, as well as an assessment of the likelihood that the postulated threat would occur.

The NIPP framework calls for CIKR partners to assess risk from any scenario as a function of consequence, vulnerability, and threat, as defined below. As stated in the introduction to this chapter, it is important to think of risk as influenced by the nature and magnitude of a threat, the vulnerabilities to that threat, and the consequences that could result:

$$R = f(C,V,T)$$

- **Consequence:** The effect of an event, incident, or occurrence; reflects the level, duration, and nature of the loss resulting from the incident. For the purposes of the NIPP, consequences are divided into four main categories: public health and safety (i.e., loss of life and illness); economic (direct and indirect); psychological; and governance/mis-mission impacts.

- **Vulnerability:** Physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. In calculating the risk of an intentional hazard, a common measure of vulnerability is the likelihood that an attack is successful, given that it is attempted.
- **Threat:** Natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. For the purpose of calculating risk, the threat of an intentional hazard is generally estimated as the likelihood of an attack being attempted by an adversary; for other hazards, threat is generally estimated as the likelihood that a hazard will manifest itself. In the case of terrorist attacks, the threat likelihood is estimated based on the intent and capability of the adversary.

CIKR-related risk assessments consider all three components of risk and are conducted on assets, systems, or networks, depending on the characteristics of the infrastructure being examined. Once the three components of risk have been assessed for one or more given assets, systems, or networks, they must be integrated into a defensible model to produce a risk estimate.

DHS conducts risk analyses for each of the 18 CIKR sectors, working in close collaboration with the SSAs, State and local authorities, and private sector owners and operators. This includes execution of the Strategic Homeland Infrastructure Risk Assessment (SHIRA) data call that provides input to risk analysis programs and projects and considers data collected more broadly through other DHS Office of Infrastructure Protection (IP) program activities as well.

DHS has identified a number of risk assessment characteristics and data requirements to produce results that enable cross-sector risk comparisons; these are termed **core criteria**. These features provide a guide for improving existing

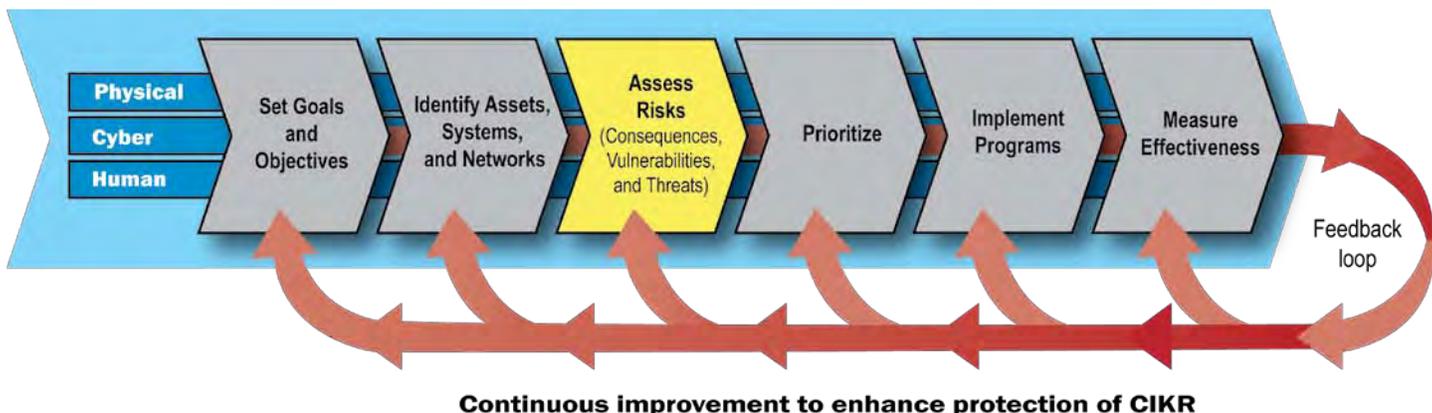
A very important program that provides a key synthesizing assessment for the Federal NIPP community is the Strategic Homeland Infrastructure Risk Assessment (SHIRA) process. The SHIRA involves an annual collaborative process conducted in coordination with interested members of the CIKR protection community to assess and analyze the risks to the Nation's infrastructure from terrorism, as well as natural and manmade hazards. The information derived through the SHIRA process feeds a number of analytic products, including the National Risk Profile, the foundation of the National CIKR Protection Annual Report, as well as individual Sector Risk Profiles.

methodologies or modifying them so that the investment and expertise they represent can be used to support national-level, comparative risk assessment, investments, incident response planning, and resource prioritization. The NIPP core criteria for risk assessments are summarized in appendix 3A and are discussed below.

3.3.1 NIPP Core Criteria for Risk Assessments

The NIPP core criteria for risk assessments identify the characteristics and information needed to produce results that can contribute to cross-sector risk comparisons. These criteria include both the analytic principles that are broadly applicable to all parts of a risk methodology and specific guidance regarding information needed to understand and address each of the three components of the risk equation: consequence, vulnerability, and threat. Risk assessments are conducted by many CIKR partners to meet their own decisionmaking needs, using a broad range of methodologies. Whenever possible, DHS seeks to use information from partners' risk assessments to contribute to an understanding of risks across sectors and throughout the Nation. Thus, adherence to the NIPP core criteria will facilitate the broadest applicability of existing assessments.

Figure 3-4: NIPP Risk Management Framework: Assess Risks



Recognizing that many risk assessment methodologies are under development and others evolve in a dynamic environment, the core criteria for risk assessment methodologies also serve as a guide to future adaptations.

The basic analytic principles ensure that risk assessments are:

- **Documented:** The methodology and the assessment must clearly document what information is used and how it is synthesized to generate a risk estimate. Any assumptions, weighting factors, and subjective judgments need to be transparent to the user of the methodology, its audience, and others who are expected to use the results. The types of decisions that the risk assessment is designed to support and the timeframe of the assessment (e.g., current conditions versus future operations) should be given.
- **Reproducible:** The methodology must produce comparable, repeatable results, even though assessments of different CIKR may be performed by different analysts or teams of analysts. It must minimize the number and impact of subjective judgments, leaving policy and value judgments to be applied by decisionmakers.
- **Defensible:** The risk methodology must logically integrate its components, making appropriate use of the professional disciplines relevant to the analysis, as well as be free from significant errors or omissions. Uncertainty associated with consequence estimates and confidence in the vulnerability and threat estimates should be communicated.
- **Complete:** The methodology should assess *consequence*, *vulnerability*, and *threat* for every defined risk scenario and follow the more specific guidance for each of these as given in the subsections that follow. The guidance is also summarized in appendix 3A.

3.3.2 Risk Scenario Identification

All risk is assessed with respect to a specific scenario or set of scenarios. Simply put, the risk scenario answers the question “The risk of what?” All consequence, vulnerability, and threat estimates are specific to the risk scenario. Risks can be assessed for assets, networks, systems, and defined combinations of these. In the case of the risk from terrorism, the subject of the risk assessment is commonly called the target. When developing scenarios for a risk assessment of a relatively fixed system, an important first step is to identify those components or critical nodes where potential consequences would be highest and where protective measures

and resiliency strategies can be focused. Open and adaptive systems are likely to require more sophisticated approaches to screening, which are still under development.

The risk scenario also identifies the potential source of harm. For terrorism, the risk scenario must include the means of attack and delivery, such as a 4000-pound TNT-equivalent, vehicle-borne improvised explosive device (VBIED). In the case of natural hazards, the risk scenario must include the type and magnitude of the hazard (e.g., a Category 5 hurricane or an earthquake of 6.5 on the Richter scale).

Finally, the scenario must identify the conditions that are relevant to calculating consequence, vulnerability, and threat. DHS uses reasonable worst-case conditions to assess terrorism risks because intelligent adversaries can choose circumstances where targets are vulnerable and consequences are maximized. The concept of “worst case” (that combination of conditions that would make the most harmful results the ones that occur) is moderated by reason. Scenarios should not be compounded in complexity to include numerous unlikely conditions, unless the focus of the contingency and other planning is on extremely rare events. Neither should scenarios be based simply on average conditions. Each type of target will have the different characteristics needed to accurately describe reasonable worst-case conditions, such as a stadium’s maximum capacity, the storage volume of a particularly hazardous material at a chemical facility, or the height and duration of a high water level at a dam.

3.3.3 Consequence Assessment

The consequences that are considered for the national-level comparative risk assessment are based on the criteria set forth in HSPD-7. These criteria can be divided into four main categories:

- **Public Health and Safety:** Effect on human life and physical well-being (e.g., fatalities, injuries/illness).⁶
- **Economic:** Direct and indirect economic losses (e.g., cost to rebuild asset, cost to respond to and recover from attack, downstream costs resulting from disruption of product or service, long-term costs due to environmental damage).
- **Psychological:** Effect on public morale and confidence in national economic and political institutions. This encompasses those changes in perceptions emerging after a significant incident that affect the public’s sense of safety and well-being and can manifest in aberrant behavior.

⁶ Injuries and illnesses are not commonly assessed at this point; however, the capability exists to develop this information and NIPP partners should move toward including it when it is relevant and possible.

- **Governance/Mission Impact:** Effect on government’s or industry’s ability to maintain order, deliver minimum essential public services, ensure public health and safety, and carry out national security-related missions.

Under the general rubric of governance/mission impact are several discrete, federally mandated missions that may be disrupted. Although many of these missions are directly fulfilled by government agencies, some are fulfilled or supported by the private sector; however, government actions can serve to either foster a healthy environment for them or inadvertently disrupt them. These include the responsibility to: ensure national security and perform other Federal missions; ensure public health; maintain order; enable the provision of essential public services; and ensure an orderly economy.

There are indirect and cascading impacts of disruptions that are difficult to understand and may be even more difficult to appraise. Some may already be accounted for in estimates of economic losses, while others may require further metrics development to enable them to be considered in a more comprehensive risk assessment. Ongoing work with NIPP partners will pursue solutions to these challenges, aiming to improve our ability to compare and prioritize mission-disruption losses in addition to the other types of consequences of concern.

A full-consequence assessment takes into consideration all four consequence criteria; however, estimating potential indirect impacts requires the use of numerous assumptions and other complex variables. An assessment of all categories of consequence may be beyond the capabilities available (or the precision needed) for a given risk assessment. At a minimum, assessments should focus on the two most fundamental impacts—the human consequences and the most relevant direct economic consequences.

3.3.3.1 Consequence Assessment Methodologies That Enable National Risk Analysis

DHS works with CIKR partners to develop or improve consequence assessment methodologies that can be applied to a variety of asset, system, or network types and to produce comparable quantitative consequence estimates. Many tools and methods can support the assessment of direct effects and consequences and are often sector-specific. Consequence analysis should ideally address both direct and indirect effects. Many assets, systems, and networks depend on connections to other CIKR to function. For example, nearly all Sectors share relationships with elements of the Energy, Information Technology, Communications, Banking and Finance, and Transportation Systems sectors. In many cases,

the failure of an asset or system in one sector will affect the ability of interrelated assets or systems in the same or another sector to perform the necessary functions. Furthermore, cyber interdependencies present unique challenges for all sectors because of the borderless nature of cyberspace. Interdependencies are dual in nature (e.g., the Energy Sector relies on computer-based control systems to manage the electric power grid, while those same control systems require electric power to operate). As a result, complete consequence analysis addresses both CIKR interconnections for the purposes of NIPP risk assessment.

Various Federal and State entities, including national laboratories, are developing sophisticated models and simulations to identify dependencies and interdependencies within and across sectors. The Federal Government established the National Infrastructure Simulation and Analysis Center (NISAC) to support these efforts (see section 6.4.2). NISAC is chartered to develop advanced modeling, simulation, and analysis capabilities for the Nation’s CIKR. These tools and analyses address dependencies and interdependencies, both physical and cyber, in an all-hazards context. These sophisticated models enhance the Nation’s understanding of CIKR dependencies and interdependencies to better inform decisionmakers, especially for cross-sector priorities.

The level of detail and specificity achieved by using the most sophisticated models and simulations may not be practical or necessary for all assets, systems, or networks. In these circumstances, a simplified dependency and interdependency analysis based on expert judgment may provide sufficient insight to make informed risk management decisions in a timely manner.

3.3.3.2 Consequence Uncertainty

There is an element of uncertainty in consequence estimates. Even when a scenario with reasonable worst-case conditions is clearly stated and consistently applied, there is often a range of outcomes that could occur. For some incidents, the consequence range is small and a single estimate may provide sufficient information to support decisions. If the range of outcomes is large, the scenario may require more specificity about conditions to obtain appropriate estimates of the outcomes. However, if the scenario is broken down to a reasonable level of granularity and there is still significant uncertainty, the single estimate should be accompanied by the uncertainty range to support more informed decisionmaking. The best way to communicate uncertainty will depend on the factors that make the outcome uncertain, as well as the amount and type of information that is available.

Core Criteria Guidance for Consequence Assessments

- Document the scenarios assessed, tools used, and any key assumptions made.
- Estimate the number of fatalities, injuries, and illnesses, where applicable and feasible, keeping each separate estimate visible to the user.
- Estimate the economic loss in dollars, stating which costs are included (e.g., property damage losses, lost revenue, loss to the economy) and what duration was considered.
- If monetizing human health consequences, document the value(s) used and the assumptions made.
- Consider and document any protective or consequence mitigation measures that have their effect after the incident has occurred, such as the rerouting of systems or HAZMAT or fire-and-rescue response.
- Describe psychological impacts and mission disruption where feasible.

3.3.4 Vulnerability Assessment

Vulnerabilities are physical features or operational attributes that render an entity open to exploitation or susceptible to a given hazard. Vulnerabilities may be associated with physical (e.g., a broken fence), cyber (e.g., lack of a firewall), or human (e.g., untrained guards) factors.

A vulnerability assessment can be a stand-alone process or part of a full risk assessment. The vulnerability assessment involves the evaluation of specific threats to the asset, system, or network under review to identify areas of weakness that could result in consequences of concern.

3.3.4.1 Vulnerability Assessment Methodologies That Enable National Risk Analysis

Many different vulnerability assessment approaches are used in the different CIKR sectors and by various government authorities. The primary vulnerability assessment methodologies used in each sector are described in the respective SSPs. The SSPs also provide specific details regarding how the assessments can be carried out (e.g., by whom and how often). The results of the vulnerability assessments need to be comparable in order to contribute to national-level, cross-sector risk analysis. As with risk assessments, vulnerability assessments should meet the same core criteria (i.e., be documented, objective, defensible, and complete) if the results are to be compared at a national, cross-sector level. In addition, vulnerability-specific core criteria guidance is provided at the end of this section.

3.3.4.2 SSA and DHS Analysis Responsibilities

SSAs and their sector partners are responsible for collecting and documenting the vulnerability assessment approaches used within their sectors. Owners or operators typically perform the vulnerability assessments, sometimes with facilitation by government authorities. The SSAs are also responsible for compiling, where possible, vulnerability assessment results for use in sector and national risk analysis efforts. In addition, the SSAs work with DHS, where possible, to review the results of assessments for assets, systems, and networks that are of greatest concern from the SSA's perspective. The SSAs should strive to involve owners and operators in this effort. Vulnerability assessment information may be submitted by owner/operators for validation as PCII under the PCII Program (see section 4.3, Protection of Sensitive CIKR Information). The PCII Program Manager may designate some information as "categorically included" PCII (see section 4.3.1, Protected Critical Infrastructure Information Program). This designation provides the SSA with the option to receive the categorically included Critical Infrastructure Information (CII) directly from the submitter. This arrangement is based on pre-approval from the PCII Program Office on a case-by-case basis.

DHS works to ensure that appropriate vulnerability assessments are performed for nationally critical CIKR. DHS works with CIKR owners and operators, the SSAs, and appropriate State and local authorities, to either perform the assessment or to verify the adequacy and relevance of previously performed assessments to support risk management decisions.

California Water System Comprehensive Review

Federal, State, and local stakeholders collaborated successfully to complete the first systems-based Comprehensive Review (CR). A systems-based CR is a cooperative government-led analysis of CIKR facilities. The California Water System CR required extensive coordination, planning, research, data collection, and outreach to State and local partners to identify critical assets and system interdependencies. DHS, in conjunction with Federal and California State partners, worked with facility owners and operators to identify critical water system assets. This system consists of 161 assets spanning 33 counties. The review determined that 40 of the 161 assets were critical assets. DHS completed 32 onsite vulnerability assessments and six Emergency Services Capabilities Assessments. DHS met with site owners and operators, California State and local law enforcement, and emergency management entities to analyze and track the gaps, potential enhancements, and protective measures that were identified and to evaluate vulnerability mitigation and grant funding effectiveness.

DHS and the SSAs collaborate to support vulnerability assessments that address the specific needs of the NIPP's approach to CIKR protection and risk management. Such assessments may:

- More fully investigate dependencies and interdependencies;
- Serve as a basis for developing common vulnerability reports that can help identify strategic needs for protective programs or R&D across sectors or subsectors;
- Fill gaps when sectors or owner/operators have not yet completed assessments and decisionmaking requires such studies immediately; and
- Test and validate new methodologies or streamlined approaches for assessing vulnerability.

In some sectors and subsectors, vulnerability assessments have never been performed or may have been performed for only a small number of high-profile or high-value assets, systems, or networks. To assist in closing this gap, DHS works with the SSAs, owners and operators, and other CIKR partners to provide the following:

- Vulnerability assessment tools that may be used as part of self-assessment processes;
- Informative reports for industrial sectors, classes of activities, and high-consequence or at-risk special event sites;
- Generally accepted risk assessment principles for major classes of activities and high-consequence or at-risk special event sites;
- Assistance in the development and sharing of industry-based standards and tools;
- Recommendations regarding the frequency of assessments, particularly in light of emergent threats;

DHS National Cybersecurity Division (NCSA) has developed the Cyber Security Vulnerability Assessment (CSVA), a flexible and scalable approach that analyzes an entity's cybersecurity posture and describes gaps and targeted considerations that can reduce overall cyber risks. It assesses the policies, plans, and procedures in place to reduce cyber vulnerability in 10 categories (e.g., access control, configuration management, physical security of cyber assets, etc.) and leverages various recognized standards, guidance, and methodologies (e.g., the International Organization for Standardization 27001, the Information Systems Audit and Control Association (ISACA) Control Objects for Information and Related Technology (COBIT), and the National Institute of Standards and Technology Special Publication 800 series).

Core Criteria Guidance for Vulnerability Assessments

- **Identify the vulnerabilities associated with physical, cyber, or human factors (openness to both insider and outsider threats), critical dependencies, and physical proximity to hazards.**
- **Describe all protective measures in place and how they reduce the vulnerability for each scenario.**
- **In evaluating security vulnerabilities, develop estimates of the likelihood of an adversary's success for each attack scenario.**
- **For natural hazards, estimate the likelihood of the incident causing harm to the asset, system, or network, given that the natural hazard event occurs at the location of interest for the risk scenario.**

- Site assistance visits and vulnerability assessments of specific CIKR as requested by owners and operators, when resources allow; and
- Cyber vulnerability assessment best practices. (DHS works to leverage established methodologies that have traditionally focused on physical vulnerabilities by enhancing them to better address cyber elements.)

Some vulnerability assessments will include both vulnerability analysis and consequence analysis for specified scenarios.

3.3.5 Threat Assessment

The remaining factor to be considered in the NIPP risk assessment process is the assessment of threat. Assessment of the current terrorist threat to the United States is derived from extensive study and understanding of terrorists and terrorist organizations, and frequently is dependent on analysis of classified information. DHS provides its partners with Federal Government-coordinated unclassified assessments of potential terrorist threats and appropriate access to classified assessments where necessary and authorized. These threat assessments are derived from analyses of adversary intent and capability, and describe what is known about terrorist interest in particular CIKR sectors, as well as specific attack methods. Since international terrorists, in particular, have continually demonstrated flexibility and unpredictability, DHS and its partners in the Intelligence Community also analyze known terrorist goals, objectives, and developing capabilities to provide CIKR owners and operators with a broad view of the potential threat and postulated terrorist attack methods.

TRIPwire Community Gateway

The *TRIPwire* Community Gateway (TWCG) is a new *TRIPwire* Web portal designed specifically for the Nation's CIKR owners, operators, and private security personnel. TWCG provides expert threat analyses, reports, and relevant planning documents to help key private sector partners anticipate, identify, and prevent improvised explosive device (IED) incidents. TWCG shares IED-related information tailored to each of the 18 sectors of CIKR. Sector partners benefit from increased communication, improved awareness of emerging threats, and access to resources and guidance on specific IED preventive and protective measures for their facilities and requirements.

3.3.5.1 Key Aspects of the Terrorist Threat to CIKR

Analysis of terrorist goals and motivations reveals that domestic and international CIKR are potentially prime targets for terrorist attack. Given the deeply rooted nature of these goals and motivations, CIKR likely will remain highly attractive targets for terrorists. Threat assessments must address the various elements of CIKR—physical, cyber, and human—depending on the attack type and target. Physical attacks, including the exploitation of physical elements of CIKR, represent the attack method most frequently used overtly by terrorists. In addition, there is increasing indication of terrorists' intent to conduct cyber attacks and exploit the knowledge, influence, and access of insiders.

3.3.6 Homeland Infrastructure Threat and Risk Analysis Center

The DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) conducts integrated threat and risk analyses for CIKR sectors. HITRAC is a joint intelligence center that spans both the DHS Office of Intelligence and Analysis (I&A)—a member of the Intelligence Community—and IP. As called for in section 201 of the Homeland Security Act, HITRAC brings together intelligence and infrastructure specialists to ensure a sufficient understanding of the risks to the Nation's CIKR from foreign and domestic threats. HITRAC works in partnership with the U.S. Intelligence Community and national law enforcement to integrate and analyze intelligence and law enforcement information in threat and risk analyses products. HITRAC also works in partnership with the SSAs and owners and operators to ensure that their expertise on infrastructure operations is integrated into HITRAC analyses.

HITRAC develops analytical products by combining threat assessments based on all-source information and intel-

ligence analysis with vulnerability and consequence assessments. This process provides an understanding of the threats, CIKR vulnerabilities, and potential consequences of attacks and other hazards. Analyses may also include potential options for managing risk. This combination of intelligence and practical CIKR knowledge allows DHS to provide products that contain strategically relevant and actionable information. It also allows DHS to identify intelligence collection requirements in conjunction with CIKR partners so that the Intelligence Community can provide the type of information necessary to support the CIKR risk management and protection missions. HITRAC coordinates closely with partners outside the Federal Government through the SSAs, SCCs, GCCs, Information Sharing and Analysis Centers (ISACs), State and Local Fusion Centers, and State Homeland Security Offices to ensure that its products are relevant to partner needs and are accessible.

3.3.6.1 Threat and Incident Information

DHS leverages, on a 24/7 basis, intelligence and operations monitoring and reporting from multiple sources to provide analyses based on the most current information available on threats, incidents, and infrastructure status. The timely analysis of information provided by DHS is of unique value to CIKR partners and helps them determine if changes are needed in steady-state and threat-based CIKR risk management measures.

Core Criteria Guidance for Threat Assessments

For adversary-specific threat assessments:

- Account for the adversary's ability to recognize the target and the deterrence value of existing security measures.
- Identify any attack methods that may be employed.
- Consider the level of capability that an adversary demonstrates for a particular attack method.
- Consider the degree of the adversary's intent to attack the target.
- Estimate threat as the likelihood that the adversary would attempt a given attack method against the target.
- If threat likelihoods cannot be estimated, use conditional risk values (consequence times vulnerability) and conduct sensitivity analyses to determine how likely the scenario would have to be to support the decision.

For natural disasters and accidental hazards:

- Use best-available analytic tools and historical data to estimate the likelihood of these events affecting CIKR.

DHS uses a variety of tools and systems to support incident and threat warnings. iCAV and DHS Earth help visualize these incident reports and threat warnings, allowing analysts to deliver a geospatial context to numerous information systems. It facilitates fusing information from multiple suspicious activity sources and provides situational awareness tracking for disasters such as hurricanes and other real-time events. This fusion provides DHS, States, local jurisdictions, and the private sector with a rapid, common understanding of the relationships between these events to support coordinated risk-mitigation, preparedness, response, and recovery activities.

DHS also supports SLFC efforts by ensuring that relevant threat information is passed along in a timely manner to SLFCs, that analyses conducted by national intelligence centers such as HITRAC are readily available to SLFC partners, and that initiatives designed to share best practices related to CIKR identification, risk analysis, and prioritization are supported.

Specialized products that directly support the NIPP and the SSPs include incident reports and threat warnings, which are made available to appropriate partners.

Incident Reports: DHS monitors information on incidents to provide reports that CIKR owners and operators and other decisionmakers can use when considering how evolving incidents might affect their CIKR protection posture. This reporting provides a responsive and credible source to verify or expand on information that CIKR partners may receive initially through the news media, the Internet, or other sources. DHS works with multiple government and private sector operations and watch centers to combine situation reports from law enforcement, intelligence, and private sector sources with infrastructure status and operational expertise to rapidly produce reports from a trusted source. These help inform the decisions of owners and operators regarding changes in risk-mitigation measures that are needed to respond to incidents in progress, such as rail or subway bombings overseas that may call for precautionary actions domestically.

Strategic Threat Assessments: HITRAC works with the Intelligence Community and with DHS's partners to analyze information on adversaries who pose a threat to CIKR. HITRAC provides a high-level assessment of terrorist groups and other adversaries to the SSAs in order to inform their SSPs and prioritization efforts.

Threat Warnings: DHS monitors the flow of intelligence, law enforcement, and private sector security information on a 24/7 basis in light of the business, operational, and status expertise provided by its infrastructure analysis and owner/operator partners to produce relevant threat warnings for CIKR protection. The fusion of intelligence and infrastructure

analysis clarifies the implications of intelligence reporting about targeted locations or sectors, potential attack methods and timing, or the specific nature of an emerging threat.

3.3.6.2 Risk Analysis

HITRAC uses risk analysis and other approaches to aid CIKR partners in identifying, assessing, and prioritizing risk management approaches. HITRAC also develops specialized products for strategic planning that directly support the NIPP and SSPs. In addition to these specific products, HITRAC produces strategic assessments and trend analyses that help define the evolving risk to the Nation's CIKR.

- **National Infrastructure Risk Analysis Program:** National, State, regional, cross-sector, sector-specific, and site-specific risk analyses and assessments aid decisionmakers with planning and prioritizing risk-reduction measures within and across the CIKR sectors. These analyses and assessments leverage a number of analytic approaches, including the SHIRA process, which are tailored to particular decisions.
- **National CIKR Prioritization Program:** HITRAC works with CIKR partners to identify and prioritize the assets, systems, and networks most critical to the Nation through the Tier 1 and Tier 2 Program for critical assets, systems, networks, nodes, and functions within the United States, and the Critical Foreign Dependencies Initiative (CFDI) for CIKR outside of the United States. The prioritization of CIKR guides the Nation's protective and incident management responses.
- **Infrastructure Risk Analysis Partnership Program (IRAPP):** IRAPP assists partners interested in pursuing their own CIKR risk analysis, whether they are in the Federal, State, local, or private sector CIKR protection communities. IRAPP involves customized support to interested partners and the sharing of best practices across the CIKR protection community.
- **Committee on Foreign Investment in the United States (CFIUS) Support:** CFIUS is an interagency committee of the Federal Government that reviews the national security implications of foreign investments of U.S. companies or operations. HITRAC provides support to CFIUS by developing written threat and risk assessments of foreign direct investment in the United States and evaluating the potential risks posed by foreign acquisition of U.S. CIKR. HITRAC also supports DHS efforts to manage those risks through the interagency CFIUS process.
- **Critical Infrastructure Red Team (CIRT):** The CIRT program focuses its analysis on high-risk sectors/subsectors and high-risk attack methods from the perspective of our Nation's adversaries by conducting open-source analysis,

developing operational plans, and exercising these scenarios through tabletop exercises and developing lessons learned from those activities. These efforts identify gaps in current strategies and risk-reduction programs for the Nation's CIKR and support the development of recommendations for closing or managing identified gaps.

- **Risk Analysis Development Program:** The Risk Analysis Development Program works to improve the capabilities available to CIKR risk analysts and risk managers, both in DHS and among the rest of the NIPP stakeholders. The program conducts R&D to identify sound, common risk analysis approaches that support cross-sector comparisons and the full range of risk management decisions. Such practices use the risk assessment core criteria summarized in appendix 3A as a foundation, but also require the use of common scenarios and assumptions. These capabilities are being tested and are evolving to overcome lingering challenges as risk analysis practices for homeland security mature.
- **Critical Foreign Dependencies Initiative (CFDI):** CFDI, as part of the larger National CIKR Prioritization Program, is the Nation's first step toward the identification and prioritization of the Nation's critical foreign dependencies. The program provides a consolidating and coordinating mechanism by which the Federal Government may more effectively and efficiently engage our foreign CIKR partners.

3.4 Prioritize

Prioritizing risk management efforts regarding the most significant CIKR helps focus planning, increase coordination, and support effective resource allocation and incident management, response, and restoration decisions.

The NIPP risk management framework is applicable to risk assessments on an asset, system, network, function, national,

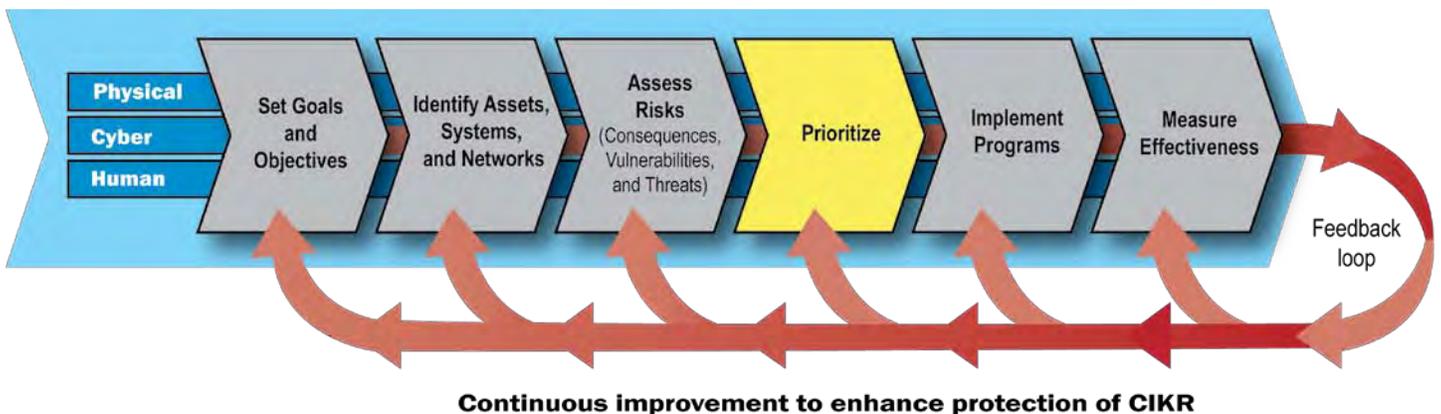
State, regional, or sector basis. Comparing the risk faced by different entities helps identify where risk mitigation is needed and to subsequently determine and help justify the most cost-effective risk management options. This approach identifies which CIKR should be given priority for risk reduction and which alternative options represent the best investment based on their risk-reduction return on investment. The prioritization process also develops information that can be used during incident response to help inform decisionmakers regarding issues associated with CIKR restoration.

3.4.1 The Prioritization Process

The prioritization process involves aggregating, combining, and analyzing risk assessment results to determine which assets, systems, networks, sectors, or combinations of these face the highest risk so that risk management priorities can be established. It also provides the basis for understanding potential risk-mitigation benefits that are used to inform planning and resource decisions.

This process involves two related activities: The first determines which regions, sectors, or other aggregation of CIKR assets, systems, or networks have the highest risk from relevant incidents or events. Of those with similar risk levels, the CIKR with the highest expected losses are accorded the highest priority in risk management program development. The second activity determines which actions are expected to provide the greatest mitigation of risk for any given investment. The risk management initiatives that result in the greatest risk mitigation for the investment proposed are accorded the highest priority in program design, resource allocation, budgeting, and implementation. Other priorities may be set based on regulatory or statutory requirements, presidential directives, and congressional mandates. This approach ensures that programs make the greatest contribution possible to overall CIKR risk mitigation given the

Figure 3-5: NIPP Risk Management Framework: Prioritize



National CIKR Prioritization Program

The DHS Tier 1 and Tier 2 Program identifies nationally significant critical assets and systems in order to enhance decision-making related to CIKR protection. CIKR identified through the program include those that, if destroyed or disrupted, could cause some combination of significant casualties, major economic losses, or widespread and long-term disruptions to national well-being and governance capacity.

The overwhelming majority of the assets and systems identified through this effort are classified as Tier 2. Only a small subset of assets meet the Tier 1 consequence threshold—those whose loss or damage could result in major national or regional impacts similar to the impacts of Hurricane Katrina or the September 11, 2001, attacks. The process of identifying these nationally significant assets and systems is conducted on an annual basis and relies heavily on the insights and knowledge of a wide array of public and private sector security partners.

CIKR categorized as Tier 1 or Tier 2 as a result of this annual process provide a common basis on which DHS and its security partners can implement important CIKR protection programs and initiatives, such as various grant programs, buffer zone protection efforts, facility assessments and training, and other activities. Specifically, the Tier 1/Tier 2 list is used to support eligibility determinations for Urban Area Security Initiative (UASI), State Homeland Security, and Buffer Zone Protection grant programs. The Tier 1/Tier 2 list is classified.

To meet the growing need for additional prioritized lists of infrastructure for planning and incident management purposes, the National CIKR Prioritization Program has also expanded to: identify, assess, and prioritize foreign infrastructure critical to the Nation through CFDI; provide sectors and States with the opportunity to build lists to meet their individual risk and incident management needs; and provide a forum through which the infrastructure protection community can and will continue to improve its ability to prioritize CIKR during incidents and enable response and recovery operations.

available resources. In light of emerging threats, the need to address current credible threat information may require shifting resources.

Assessments become more complex and difficult at different aggregations, such as when comparisons are necessary across sectors, across different geographic areas, or against different types of events. Using a common approach with consistent assumptions and metrics increases the ability to make such comparisons. Without this consistency, assessments are much more challenging.

3.4.2 Tailoring Prioritization Approaches to Sector and Decisionmakers' Needs

CIKR partners rely on different approaches to prioritize risk management activities according to their authorities, specific sector needs, risk landscapes, security approaches, and business environment. For example, owners and operators, Federal agencies, and State and local authorities all have different options available to them to help reduce risk. Asset-focused priorities may be appropriate for CIKR whose risk is predominantly associated with facilities, the local environment, and physical attacks, especially those that can be exploited and used as weapons. Function-focused priorities may more effectively ensure the continuity of operations in the event of a terrorist attack or natural disaster in sectors where CIKR resilience may be more important than CIKR hardening. Programs to reduce CIKR risk give priority to investments that protect physical assets or ensure resilience in virtual systems, depending on which option best enables cost-effective CIKR risk management.

To ensure a consistent approach to risk analysis for CIKR protection, partners establish priorities using risk analyses that use common scenarios and assumptions and follow the parameters for risk assessment methodologies set out in appendix 3A. For quick-response decisions, lacking

Critical Foreign Dependencies Initiative

CFDI involves three phases of activities, two on an annual basis and one ongoing:

- Phase I—Identification (annual): DHS, working with CIKR protection and intelligence community partners, developed the first-ever National Critical Foreign Dependencies List in FY2008, reflecting the critical foreign dependencies of the CIKR sectors, as well as critical foreign dependencies of interest to the Nation as a whole. The identification process includes input from public and private sector CIKR partners.
- Phase II—Prioritization (annual): DHS, working with CIKR partners, and in particular DOS, prioritized the National Critical Foreign Dependencies List based on factors such as the overall criticality of the CIKR to the United States and foreign partner willingness and capability to engage in collaborative risk management activities.
- Phase III—Engagement (ongoing): Phase III involves leveraging the prioritized National Critical Foreign Dependencies List to guide current and future U.S. bilateral and multilateral incident and risk management activities with foreign partners. DHS and DOS established mechanisms to ensure coordinated engagement and collaboration by public sector entities, in partnership with the private sector.

sound risk assessments for reference, some priorities will be informed by top-down assessments using surrogate data or data at high levels of CIKR aggregation (e.g., population density as a surrogate for casualties). As both the NIPP partnership and the knowledge base of risk assessments grow, decisions can be increasingly informed by a combination of top-down and bottom-up analyses using detailed information on specific individual facilities, with a prioritization based on the level of risk reduced by the investment.

3.4.3 The Uses of Prioritization

A primary use of prioritization is to inform resource allocation decisions, such as: where risk management programs should be instituted; guidance on investments in these programs; and which measures offer the greatest return on investment. The results of the prioritization process guide CIKR risk management requirements and should drive important resource allocation decisions.

At the national level, DHS is responsible for overall national risk-informed CIKR prioritization in close collaboration with the SSAs, States, and other CIKR partners. SSA responsibilities include managing government interaction with the sector and helping to cultivate information sharing and collaboration to identify, prioritize, and manage risk. They must also extend their sector focus to enable cross-sector comparisons of risk and metrics that help owners and operators, as well as Federal, State, local, and tribal governments, support evaluations of the risk-reduction return on various investments. At the State level, DHS is working to develop a collaborative relationship with State and local authorities through the Infrastructure Risk Analysis Partnership Program. This effort is geared toward working with State authorities to foster the capability to develop, evaluate, and support the implemen-

The National CIKR Risk Profile

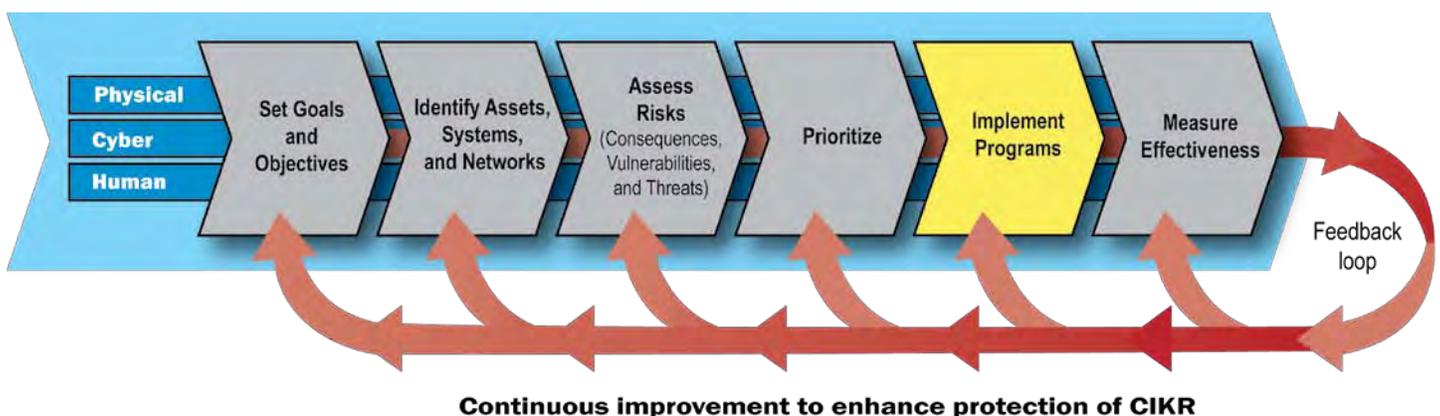
Leveraging information provided through the SHIRA process, HITRAC produces a National CIKR Risk Profile that serves as the foundation of the infrastructure protection community's common prioritization of risks to the Nation's infrastructure and is captured in the National CIKR Protection Annual Report. Each year, the National Risk Profile identifies the highest relative risks to CIKR from among a number of natural and manmade hazards, as well as those sectors at a higher risk from the greatest number of hazards. The report also identifies additional risk management concerns, such as high-likelihood risks and low-likelihood/high-consequence infrastructure protection priorities. By providing a common understanding of the Nation's CIKR risks, the National Risk Profile provides a common basis for prioritization and helps to focus community efforts on those hazards and sectors of greatest overall concern.

tation of CIKR risk management decisions in a State/local environment. The program is initially being piloted with a limited group of CIKR partners and will subsequently be rolled out more broadly as the roles, responsibilities, and approaches are tested and refined.

3.5 Implement Protective Programs and Resiliency Strategies

The risk assessment and prioritization process at the sector and jurisdictional levels will help identify requirements for near-term and future protective programs and resiliency strategies. Some of the identified shortfalls or opportunities for improvement will be filled by owner/operators, either voluntarily or based on various incentives. Other shortfalls will be addressed

Figure 3-6: NIPP Risk Management Framework: Implement Programs



through the protective programs that each sector develops under the SSP, in State CIKR protection plans, or through cross-sector or national initiatives undertaken by DHS.

The Nation's CIKR is widely distributed in both a physical and logical sense. Effective CIKR protection requires both distributed implementation of protective programs by partners and focused national leadership to ensure implementation of a comprehensive, coordinated, and cost-effective approach that helps reduce or manage the risks to the Nation's most critical assets, systems, and networks. At the implementation level, protective programs and resiliency strategies consist of numerous, diverse actions that are undertaken by various CIKR partners. From the leadership perspective, programs are structured to address coordination and cost-effectiveness.

The following sections describe the nature and characteristics of best practice protective programs and resiliency strategies, as well as some existing programs that could be applied to specific assets, systems, and networks.

3.5.1 Risk Management Actions

Risk management actions involve measures designed to: prevent, deter, and mitigate the threat; reduce vulnerability to an attack or other disaster; minimize consequences; and enable timely, efficient response and restoration in a post-event situation, whether a terrorist attack, natural disaster, or other incident. The NIPP risk management framework focuses attention on those activities that bring the greatest return on investment, not simply the vulnerability reduction to be achieved. Protective programs and resiliency strategies vary between sectors and across a wide spectrum of activities designed to deter, devalue, detect, or defend.

Risk management actions also may include the means for mitigating the consequences of an attack or incident. These actions are focused on mitigation, response, and/or recovery. Generally, it is considered more cost-effective to build security and resiliency into assets, systems, and networks than to retrofit them after initial development and deployment. Accordingly, CIKR partners should consider how risk management, robustness, resiliency, and appropriate physical security and cybersecurity enhancements could be incorporated into the design and construction of new CIKR.

In situations where robustness and resiliency are keys to CIKR protection, providing protection at the system level rather than at the individual asset level may be more effective and efficient (e.g., if there are many similar facilities, it may be easier to allow other facilities to provide the infrastructure service rather than to protect each facility).

3.5.2 Characteristics of Effective Protective Programs and Resiliency Strategies

Characteristics of effective CIKR protective programs and resiliency strategies include, but are not limited to, the following:

- **Comprehensive:** Effective programs must address the physical, cyber, and human elements of CIKR, as appropriate, and consider long-term, short-term, and sustainable activities. The SSPs describe many programs and initiatives to protect CIKR within the sector (e.g., operational changes, physical protection, equipment hardening, cyber protection, system resiliency, backup communications, training, response plans, and security system upgrades).
- **Coordinated:** Because of the highly distributed and complex nature of the various CIKR sectors, the responsibility for protecting CIKR must be coordinated:
 - CIKR owners and operators (public or private sector) are responsible for protecting property, information, and people through measures that manage risk to help ensure more resilient operations and more effective loss prevention. These measures include increased awareness of terrorist threats and implementation of operational responses to reduce vulnerability (e.g., changing daily routines, keeping computer software and virus-checking applications up to date, and applying fixes for known software defects).
 - State, local, and tribal authorities are responsible for providing or augmenting protective actions for assets, systems, and networks that are critical to the public within their jurisdiction and authority. They develop protective programs, supplement Federal guidance and expertise, implement relevant Federal programs such as the Buffer Zone Protection Program (BZPP), and provide specific law enforcement capabilities as needed. When appropriate, they have access to Federal resources to meet jurisdictional protection priorities.
 - Federal agencies are responsible for enabling or augmenting protection for CIKR that is nationally critical or coordinating the efforts of CIKR partners and the use of resources from different funding sources. DHS, SSAs, and other Federal departments and agencies carry out these responsibilities while respecting the authorities of State, local, and tribal governments, and the prerogatives of the private sector.
 - The SSAs, in conjunction with sector partners, provide information on the most effective long-term protection

strategies, develop protective programs, and coordinate the implementation of programs for their sectors. For some sectors, this includes the development and sharing of best and effective practices and related criteria, guidance documents, and tools.

- DHS, in collaboration with the SSAs and other public and private sector partners, serves as the national focal point for the development, implementation, and coordination of risk management approaches and tools and of protective programs and resiliency strategies (including cybersecurity efforts) for those assets that are deemed to be nationally critical.
- **Cost-Effective:** Effective CIKR programs and strategies seek to use resources efficiently by focusing on actions that offer the greatest mitigation of risk for any given expenditure. The following is a discussion of factors that should be considered when assessing the cost-effectiveness and public benefits derived through implementation of CIKR protection initiatives:
 - Operating with full information: The NIPP describes the mechanisms that enable the use of information regarding threats and corresponding protective actions. These mechanisms include: information sharing; provision of a dedicated communications network; and the use of established, interoperable industry and trade association communications mechanisms.
 - Addressing the present-future tradeoff in long-lead-time investments: The NIPP provides the processes and coordinating structures that allow State, local, and tribal governments and private sector partners to effectively use long-lead-time approaches to CIKR protection.
 - Matching the underlying economic incentives of each CIKR partner to the full extent possible: The NIPP supports market-based economic incentives wherever possible by relying on CIKR partners to undertake those efforts that are in their own interests and complementing those efforts with additional resources where necessary and appropriate. This coordinated approach builds on existing efforts that have proven to be effective and that are consistent with best business practices, such as owners and operators selecting the measures that are best suited to their particular risk profile and needs.
 - Addressing the public-interest aspects associated with CIKR protection: Risk management actions for CIKR that provide benefits to the public at large go beyond the actions that benefit owners and operators, or even those that benefit the public residing in a particular State,

locality, or region. Such additional actions reflect different levels of the public interest—some CIKR are critical to the national economy and to national well-being; some CIKR are critical to a State, locality, or region; some CIKR are critical only to the individual owner/operator or direct customer base. Actions to protect the public's interest that require investment beyond the level that those directly responsible for protection are willing and able to provide must be of sufficient priority to warrant the use of the limited resources that can be provided from public funding or may require regulatory action or appropriate incentives to encourage the private sector to undertake them.

- **Risk-Informed:** Protective programs and resiliency strategies focus on mitigating risk. Associated actions should be designed to allow measurement, evaluation, and feedback based on risk mitigation. This allows owners, operators, and the SSAs to reevaluate risk after the program has been implemented. These programs and strategies use different mechanisms for addressing each element of risk and combine their effects to achieve overall risk mitigation. These mechanisms include:
 - Consequences: Protective programs and resiliency strategies may limit or manage consequences by reducing the possible loss resulting from a terrorist attack or other disaster through redundant system design, backup systems, and alternative sources for raw materials or information.
 - Vulnerability: Protective programs may reduce vulnerability by decreasing the susceptibility to destruction, incapacitation, or exploitation by correcting flaws or strengthening weaknesses in assets, systems, and networks.
 - Threat: Protective programs and resiliency strategies indirectly reduce threat by making assets, systems, or networks less attractive targets to terrorists by lessening their vulnerability and lowering the consequences. As a result, terrorists may be less likely to achieve their objectives and, therefore, less likely to focus on the CIKR in question.

3.5.3 Risk Management Activities, Initiatives, and Reports

DHS, in collaboration with the SSAs and other sector partners, undertakes a number of protective programs, resiliency strategies, initiatives, activities, and reports that support CIKR protection. Many of these are available to or provide resources for CIKR partners. These activities span a wide range of efforts that include, but are not limited to, the following:

IP Vulnerability Assessment Project

The IP Vulnerability Assessment (VA) Project serves as the focal point for strategic planning, coordination, and information sharing in conducting vulnerability assessments of the Nation's Tier 1 and Tier 2 CIKR. Through the development and deployment of a scalable assessment methodology, the VA Project supports the implementation of the NIPP through identifying vulnerabilities, supporting collaborative security planning, and recommending protective measures strategies. IP VA Project initiatives include the BZPP, Site Assistance Visits (SAVs), CRs, and the Computer-Based Assessment Tool (CBAT). The VA Project provides vulnerability assessment methodologies that enhance DHS's and CIKR stakeholders' ability to prevent, protect, and respond to terrorist attacks and all-hazards incidents. The VA Project brings together: Federal, State, local, tribal, and territorial governments; local law enforcement; emergency responders; and CIKR owner and operators to conduct assessments to identify critical assets, vulnerabilities, consequences, and protective measures and resiliency strategies. The VA Project also provides analysis of CIKR facilities to include: potential terrorist actions for an attack; the consequences of such an attack; and the integrated preparedness and response capabilities of Federal, State, local, tribal, and territorial and private sector partners. The results are used to enhance the overall CIKR protection posture at the facility, community, and regional levels using short-term enhancements and long-term risk-informed investments in training, processes, procedures, equipment, and resources.

- **Buffer Zone Protection Program:** A Federal grant program designed to provide resources to State and local law enforcement to enhance the protection of a given critical facility.
- **Assistance Visits:** Facility security assessments jointly conducted by a federally led team and facility owners and operators that are designed to facilitate vulnerability identification and mitigation discussions with individual owners and operators.
- **Training Programs:** Training programs are designed to provide CIKR partners with a source from which they can obtain specialized training to enhance CIKR protection. Subject matter, course length, and location of training can be tailored to the partner's needs.
- **Control System Security:** DHS coordinates efforts among Federal, State, local, and tribal governments, as well as control system owners, operators, and vendors to improve control system security within and across all CIKR sectors.

- **Multi-Jurisdictional Improvised Explosive Device Security Plans:** DHS assists high-risk urban environments with developing thorough IED security plans that efficiently integrate assets and capabilities from multiple jurisdictions and emergency services disciplines. The plan that results from this process can help determine what actions are necessary to enhance IED prevention and the protection capabilities of the multi-jurisdictional area, which ultimately culminates in the development of a NRF- and National Incident Management System (NIMS)-compliant multi-jurisdictional plan.
- **Protective Security Advisor (PSA) Program:** DHS CIKR protection and vulnerability assessment specialists are assigned as liaisons between DHS and the CIKR protection community at the State, local, and private sector levels in geographical areas representing major concentrations of CIKR across the United States. PSAs are responsible for sharing risk information and providing technical assistance to local law enforcement and owners and operators of CIKR within their respective areas of responsibility. The PSA Duty Desk serves as the conduit among the PSAs, DHS, and other CIKR partners to facilitate, on a 24/7 basis, coordination and collaboration during steady-state and incident operations.

Protective Security Advisors

The mission of the PSAs is to represent DHS and IP in local communities throughout the United States. PSAs work with State HSAs, acting as liaisons among: DHS; the private sector; and Federal, State, local, tribal, and territorial entities and serving as DHS locally based critical infrastructure protection specialists. PSAs provide support to officials responsible for special events planning and exercises, and provide real-time information on facility significance and protective measures to facility owners and operators, as well as State and local representatives. PSAs assist and facilitate IP efforts to identify, assess, monitor, and minimize risk to CIKR at the State, local, and regional levels.

As a result of their national "footprint" across the United States, PSAs are often the first department personnel to provide support for emergent incidents. Consequently, PSAs are uniquely able to provide early situational awareness to DHS and IP leadership during an incident or contingency operations. During natural disasters and contingencies, PSAs deploy to State and local Emergency Operations Centers (EOCs) and SLFCs to provide situational awareness and facilitate information exchange to and from the field. During incidents, upon designation by the Assistant Secretary of Infrastructure Protection, PSAs perform as Infrastructure Liaisons (ILs) at Joint Field Offices (JFOs) in support of the Principal Federal Officials (PFOs) and Federal Coordinating Officers (FCOs) under the NRF.

A detailed discussion of DHS-supported programs is provided in appendix 3B.

The SSAs and other Federal departments and agencies also oversee programs, initiatives, and activities that support CIKR protection and resiliency. Many of these are also available to or provide resources for CIKR partners. Examples include:

- The Department of Veterans Affairs created a methodology also used by the Smithsonian Institution and adapted by Federal Emergency Management Agency (FEMA) Manual 452, Risk Management: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings, to assess the risk to and mitigation for hundreds of buildings and museums.
- DOT manages a Pipeline Safety grant program that supports efforts to develop and maintain State natural gas, liquefied natural gas, and hazardous liquid pipeline safety programs.
- Other risk management activities include developing and providing informational reports, such as the DHS Characteristics of Common Vulnerabilities Reports and the Indicators of Terrorist Activity Reports, which are available to all State and territorial homeland security offices. In addition to threat and vulnerability information, informational reports also include best practices for protection measures. One report in particular, a part of FEMA’s Risk Management Series, addresses the protection of buildings and is applicable across sectors.

3.6 Measure Effectiveness

The use of performance metrics is a critical step in the NIPP risk management process to enable DHS and the SSAs to objectively and quantitatively assess improvements in CIKR protection and resiliency at the sector and national levels. While the results of risk analyses outlined in section 3.3

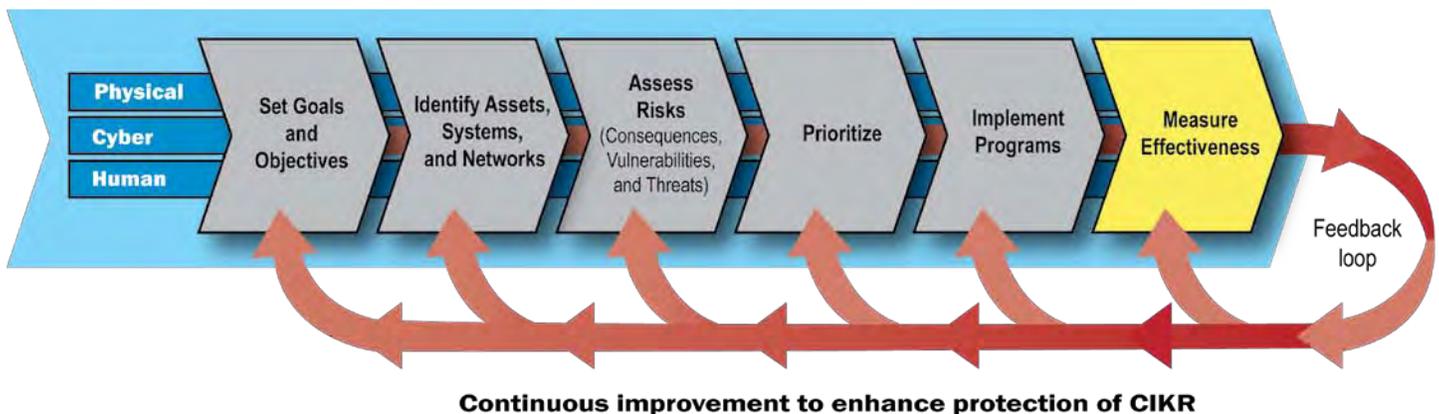
Enhanced Critical Infrastructure Protection (ECIP) Program

PSAs were directed to form partnerships with the owners and operators of the Nation’s Tier 1 and Tier 2 CIKR and conduct site visits (ECIP visits) for all of these assets. PSAs coordinate site visits with the SSAs, owners and operators, HSAs, FBI, local law enforcement (LLE), and other CIKR partners, as necessary. During the visit, PSAs document information on the facility’s current CIKR protection posture and overall security awareness. The primary goals for ECIP site visits are to:

- Inform facility owners and operators of the importance of their facilities as an identified high-priority CIKR and the need to be vigilant in light of the ever-present threat of terrorism;
- Identify protective measures currently in place at Tier 1 and Tier 2 facilities, provide comparisons of CIKR protection postures across like assets, and track the implementation of new protective measures; and
- Enhance existing relationships between Tier 1/Tier 2 facility owners and operators, DHS, and various Federal, State, local, tribal, and territorial partners in order to:
 - Provide increased situational awareness regarding potential threats;
 - Maintain an indepth knowledge of the current CIKR protection posture at each facility; and
 - Provide a known and available Federal resource to facility owners and operators.

help sectors set priorities, performance metrics allow NIPP partners to track progress against these priorities. The metrics provide a basis for DHS and the SSAs to establish accountability, document actual performance, facilitate diagnoses, promote effective management, and provide a feedback mechanism to decisionmakers.

Figure 3-7: NIPP Risk Management Framework: Measure Effectiveness



3.6.1 NIPP Metrics Types and Progress Indicators

3.6.1.1 Outcome Metrics

The focus of the NIPP metrics program is to track progress toward a strategic goal by measuring beneficial results or outcomes. The key to NIPP performance management is to align outcome metrics to sector priorities. The 18 sectors are diverse, operate in every State, and affect every level of government. As a result, NIPP priorities and many NIPP metrics will vary from sector to sector. All NIPP metrics must be specific and clear as to what they are measuring, practical or feasible in that the needed data are available, and built on objectively measured data.

In addition to outcome metrics, other information will be utilized, such as output data and descriptive data.

- *Output (or Process) Data* are used to gauge whether specific activities were performed as planned, track the progress of a task, or report on the output of a process. Output data show progress toward performing the activities necessary to achieve CIKR protection goals and can serve as leading indicators for outcome measures. They also help build a comprehensive picture of CIKR protection status and activities. Examples include the number of protective programs implemented in a fiscal year, percentage of sector organizations exchanging CIKR information, and the level of response to a data call for asset information.
- *Descriptive Data* are used to understand sector resources and activities, but do not reflect CIKR protection performance. Examples include: a narrative description of progress; the number of facilities in a jurisdiction; the population resident or working in the area affected by an incident; and the number of suppliers in an infrastructure service provider's supply chain.

NIPP metrics are evolving from the current focus on descriptive and output data to a focus on outcome metrics. Descriptive and output data have been critical during the initial implementation of the NIPP in order to closely track the progress of the sectors in building key NIPP elements, such as the SSPs and GCCs/SCCs. The next stage of NIPP implementation will concentrate on working with the sectors to identify and track outcome metrics that are aligned to sector priorities and provide NIPP partners with a more comprehensive assessment of the success of CIKR protection efforts.

3.6.1.2 NIPP Metrics Progress Indicators

NIPP outcome metrics and output/descriptive data will be identified and reported in two ways—the National Coordinator Progress Indicator and Sector Progress Indicators:

The **National Coordinator Progress Indicator** describes IP efforts to support NIPP- and SSP-related activities.

Sector Progress Indicators collectively describe the progress made by each sector and the effectiveness of different activities within the CIKR sectors.

Both types of progress indicators will have certain common features. They will contain a limited number of prioritized metrics and data that are aligned to sector priorities. Outcome metrics will be given the most importance, but some process and descriptive data may be included. Collectively, these metrics and data will provide a holistic picture of the health and effectiveness of the national and sector CIKR efforts and will help drive future investment and resource decisions.

3.6.1.3 Qualitative Information

Although not considered metrics, the NIPP also provides mechanisms for qualitative feedback that can be applied to augment and improve the effectiveness and efficiency of public and private sector CIKR protection and resiliency programs. DHS works with CIKR partners to identify and share lessons learned and best practices for all aspects of the risk management process. DHS also works with the SSAs to share relevant input from sector partners and other sources that can be used as part of the national effort to continuously improve CIKR protection and resiliency.

3.6.2 Gathering Performance Information

DHS works with the SSAs and sector partners to gather the information necessary to measure the level of performance associated with the progress indicators. Given the inherent differences in CIKR sectors, a one-size-fits-all approach to gathering this information is not appropriate. One of the available resources to support information gathering is the PSA Program through the ECIP/Infrastructure Survey Tool. The PSAs can be particularly helpful in gathering information at individual facilities or assets when different CIKR protection initiatives are implemented. This information can be used independently or combined with that of other assets, as well as with data on systems and networks that may not be amenable to physical inspection.

DHS also works with the SSAs and sector partners to determine the appropriate measurement approach to be included in the sector's SSP and to help ensure that partners engaged with multiple sectors or in cross-sector matters are not subject to unnecessary redundancy or conflicting guidance in information collection. Information collected as part of this effort is protected as discussed in detail in chapter 4.

3.6.3 Assessing Performance and Reporting on Progress

HSPD-7 requires each SSA to provide the Secretary of Homeland Security with an annual report on their efforts to identify, prioritize, and coordinate the protection of CIKR in their respective sectors. The reports are due no later than June 1 of each year. The SSAs work in close collaboration with sector partners, their respective SCCs and GCCs, and other organizations in developing this report. DHS and SSAs work in close collaboration to assess progress made toward goals in each sector based on these reports.

The National Annual Report currently includes similar reports for the SLTTGCC and the RCCC as appendixes. Additional appendixes to the current National Annual Report address the year's accomplishments for IP, the Office of Cybersecurity & Communications, the Tier 1 and Tier 2 Program, and the NISAC.

DHS compiles all of these reports into a national cross-sector report that describes annual progress toward CIKR protection goals on a national basis and makes recommendations to the EOP for prioritized resource allocation across the Federal Government to meet national CIKR protection requirements. A more detailed discussion of the national resource allocation process for CIKR protection is included in chapter 7.

In addition to these annual reports, the SSAs regularly update their measurements of CIKR status and protection levels to support DHS status tracking and comprehensive inventory updating. By maintaining a regularly updated knowledge base, DHS is able to quickly compile real-time CIKR status and protection postures to respond to changing circumstances as indicated by tactical intelligence assessments of terrorist threats or natural disaster damage assessments. This

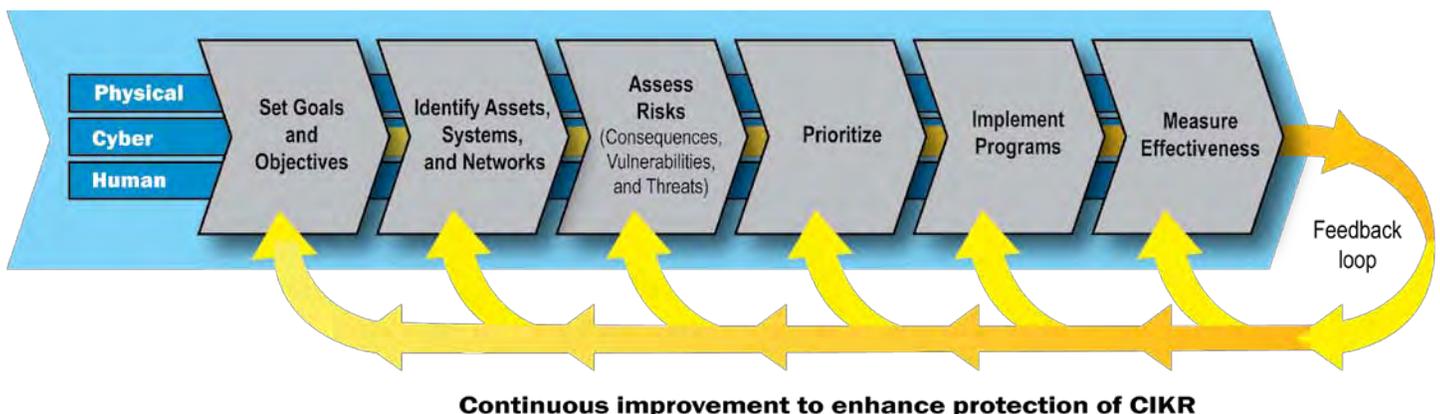
helps inform resource allocation decisions during incident response and other critical operations that support the homeland security mission.

3.7 Using Metrics and Performance Measurement for Continuous Improvement

By using NIPP metrics to evaluate the effectiveness of efforts to achieve sector priorities, CIKR partners adjust and adapt the Nation's CIKR protection approach to account for progress achieved, as well as for changes in the threat and other relevant environments. At the national level, NIPP metrics are used to focus attention on areas of CIKR protection that warrant additional government resources or other changes through an analysis of gaps and priorities for protective programs at both the national and sector levels. If an evaluation of the effectiveness of efforts to achieve priorities using NIPP metrics reveals that there is insufficient progress, DHS and its CIKR partners will undertake actions to focus efforts on addressing these particular gaps or improvement opportunities.

In addition to supporting the evaluation of progress against sector priorities, metrics can also serve as a feedback mechanism for other parts of the NIPP risk management framework. The metrics can inform progress against the broader sector goals (see section 3.1). Metrics can also provide analysts with information to adjust their risk assessments (see section 3.3). For instance, metrics indicate the effectiveness of protective programs and the extent to which these programs are mitigating risks. Finally, metrics can also inform the prioritization process (see section 3.4), as this information can assist decisionmakers in identifying effective ways to achieve desired outcomes.

Figure 3-8: NIPP Risk Management Framework: Feedback Loop for Continuous Improvement of CIKR Protection



4. Organizing and Partnering for CIKR Protection

The enormity and complexity of the Nation’s CIKR, the distributed character of our national protective architecture, and the uncertain nature of the terrorist threat and manmade or natural hazards make the effective implementation of protection and resiliency efforts a great challenge. To be effective, the NIPP must be implemented using organizational structures and partnerships committed to sharing and protecting the information needed to achieve the NIPP goal and supporting objectives described in chapter 1. DHS, in close collaboration with the SSAs, is responsible for overall coordination of the NIPP partnership organization and information-sharing network.

4.1 Leadership and Coordination Mechanisms

The coordination mechanisms described below establish linkages among CIKR protection efforts at the Federal, State, regional, local, tribal, territorial, and international levels, as well as between public and private sector partners. In addition to direct coordination, the structures described below provide a national framework that fosters relationships and facilitates coordination within and across CIKR sectors:

- **National-Level Coordination:** IP facilitates overall development of the NIPP and the SSPs, provides overarching guidance, and monitors the full range of associated coordination activities and performance measures. IP will support, not duplicate, SSA coordination, protection, or other risk reduction capabilities. Chapter 2 details specific roles for DHS.
- **Sector Partnership Coordination:** The CIKR Cross-Sector Council; the Government Cross-Sector Council (made up of two subcouncils—the NIPP Federal Senior Leadership Council (FSLC) and the SLTTGCC); and individual SCCs and GCCs create a structure through which representative

groups from Federal, State, local, and tribal governments and the private sector can collaborate and develop consensus approaches to CIKR protection.

- **Regional Coordination:** Regional partnerships, groupings, and governance bodies such as the Great Lakes Partnership, the All-Hazards Consortium, the Pacific NorthWest Economic Region, and the Southeast Regional Research Initiative enable CIKR protection coordination within and across geographical areas and sectors. Such bodies are composed of representatives from industry and State, local, and tribal entities located in whole or in part within the planning area for an aggregation of high-risk targets, urban areas, or cross-sector groupings. They facilitate enhanced coordination among jurisdictions within a State where CIKR cross multiple jurisdictions, and help sectors coordinate with multiple States that rely on a common set of CIKR. They also are organized to address common approaches to a wide variety of natural or manmade hazards. The RCCC was established in 2008 to help enhance the engagement of regionally based partners and to leverage the CIKR protection activities and resiliency strategies that they lead.

- **International Coordination:** The United States-Canada-Mexico Security and Prosperity Partnership; the North Atlantic Treaty Organization’s (NATO’s) Senior Civil Emergency Planning Committee; certain government councils, such as the CFIUS; the CFDI; and consensus-based nongovernmental or public-private organizations, such as the global Forum of Incident Response and Security Teams (FIRST), enable a range of CIKR protection coordination activities associated with established international agreements.

4.1.1 National-Level Coordination

Respecting the SSA’s responsibilities as the sector lead, DHS, in collaboration with the SSAs and the GCCs, monitors the coordination and integration of national-level CIKR protection activities through IP. In support of CIKR partner coordination, DHS:

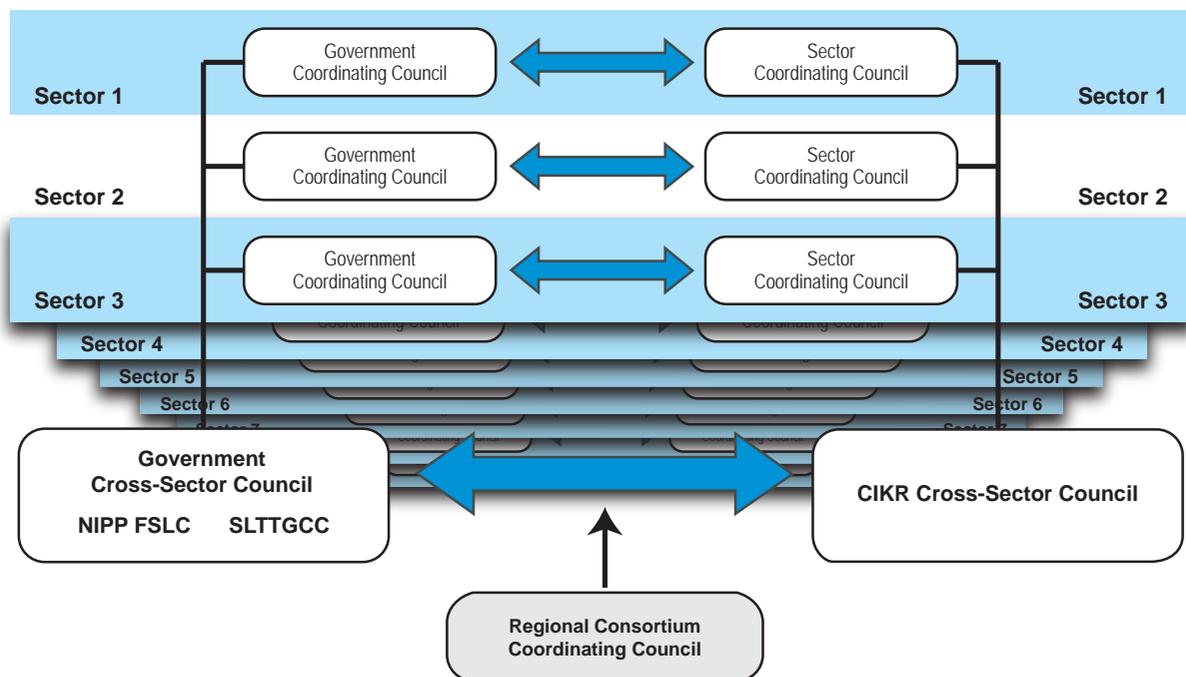
- Leads, integrates, and coordinates the execution of the NIPP, in part by acting as a central clearinghouse for the information-sharing, reporting, and coordination activities of the individual sector governance structures;
- Facilitates the development and ongoing support of governance and coordination structures or models;
- Facilitates NIPP revisions and updates using a comprehensive national review process;

- Ensures that effective policies, approaches, guidelines, and methodologies regarding partner coordination are developed and disseminated to enable the SSAs and other partners to carry out NIPP responsibilities;
- Facilitates the development of risk, risk-informed, and criticality-based assessments and prioritized lists of CIKR;
- Facilitates the sharing of CIKR prioritization and protection-related best practices and lessons learned;
- Facilitates participation in preparedness activities, planning, readiness exercises, and public awareness efforts; and
- Ensures cross-sector coordination with the SSAs to avoid conflicting guidance, duplicative requirements, and reporting.

4.1.2 Sector Partnership Coordination

The goal of NIPP-related organizational structures, partnerships, and information-sharing networks is to establish the context, framework, and support for activities required to implement and sustain the national CIKR protection effort. DHS, in collaboration with the SSAs and sector partners, issues coordinated guidance on the framework for CIKR public-private partnerships, as well as metrics to measure their effectiveness.

Figure 4-1: Sector Partnership Model



The NIPP relies on a partnership model, illustrated in figure 4-1, as the primary organizational structure for coordinating CIKR efforts and activities. The NIPP partnership model encourages formation of SCCs and GCCs as described below. DHS also provides guidance, tools, and support to enable these groups to work together to carry out their respective roles and responsibilities. SCCs and corresponding GCCs work in tandem to create a coordinated national framework for CIKR protection and resiliency within and across sectors. The sector partnership model facilitates the integration of all partners into CIKR planning and operational activities to help ensure a collaborative approach to CIKR protection.

4.1.2.1 CIKR Cross-Sector Council

Cross-sector issues and interdependencies are addressed among the SCCs through the CIKR Cross-Sector Council, which comprises the leadership of each of the SCCs. The Partnership for Critical Infrastructure Security provides this representation with support from DHS’s CIKR Executive Secretariat. The partnership coordinates cross-sector initiatives to support CIKR protection by identifying legislative issues that affect such initiatives and by raising awareness of issues in CIKR protection. The primary activities of the CIKR Cross-Sector Council include:

- Providing senior-level, cross-sector strategic coordination through partnership with DHS and the SSAs;
- Identifying and disseminating CIKR protection best practices across the sectors;
- Participating in coordinated planning efforts related to the development, implementation, and revision of the NIPP and the SSPs or aspects thereof; and
- Coordinating with DHS to support efforts to plan and execute the Nation’s CIKR protection mission.

4.1.2.2 Government Cross-Sector Council

Cross-sector issues and interdependencies between the GCCs will be addressed through the Government Cross-Sector Council, which comprises two subcouncils—the NIPP FSLC and the SLTTGCC:

- **NIPP Federal Senior Leadership Council:** The objective of the NIPP FSLC is to facilitate enhanced communications and coordination between and among Federal departments and agencies with a role in implementing the NIPP and HSPD-7. The council’s primary activities include:
 - Forging consensus on CIKR risk management strategies;
 - Evaluating and promoting implementation of risk management-based CIKR programs;

- Coordinating strategic issues and issue management resolution among Federal departments and agencies, and State, regional, local, tribal, and territorial partners;
- Advancing collaboration within and across sectors;
- Advancing collaboration with the international community;
- Participating in planning efforts related to the development, implementation, update, and revision of the NIPP and the SSPs or aspects thereof; and
- Evaluating and reporting on the progress of Federal CIKR protection activities.

- **State, Local, Tribal, and Territorial Government Coordinating Council:** The SLTTGCC serves as a forum to ensure that State, local, and tribal homeland security partners are fully integrated as active participants in national CIKR protection efforts and to provide an organizational structure to coordinate across jurisdictions on State and local government-level CIKR protection guidance, strategies, and programs. The SLTTGCC will provide the State, local, tribal, or territorial perspective or feedback on a wide variety of CIKR issues. The primary functions of the SLTTGCC include the following:

- Providing senior-level, cross-jurisdictional strategic communications and coordination through partnership with DHS, the SSAs, and CIKR owners and operators;
- Participating in planning efforts related to the development, implementation, update, and revision of the NIPP and SSPs or aspects thereof;
- Coordinating strategic issues and issue management resolution among Federal departments and agencies, and State, local, tribal, and territorial partners;
- Coordinating with DHS to support efforts to plan, implement, and execute the Nation’s CIKR protection mission; and
- Providing DHS with information on State-, local-, tribal-, and territorial-level CIKR protection initiatives, activities, and best practices.

The cross-sector bodies described in sections 4.1.2.1 and 4.1.2.2 will convene in joint session and/or working groups, as appropriate, to address cross-cutting CIKR protection issues. The NIPP-related functions of the cross-sector bodies include activities to:

- Provide or facilitate coordination, communications, and strategic-level information sharing across sectors and between and among DHS, the SSAs, the GCCs and other

supporting Federal departments and agencies, and other public and private sector partners;

- Identify issues shared by multiple sectors that would benefit from common investigations and/or solutions;
- Identify and promote best practices from individual sectors that have applicability to other sectors;
- Contribute to cross-sector information-sharing, planning, and risk management activities, as appropriate; and
- Provide input to the government on R&D efforts that would benefit multiple sectors.

4.1.2.3 Sector Coordinating Councils

The sector partnership model encourages CIKR owners and operators to create or identify an SCC as the principal entity for coordinating with the government on a wide range of CIKR protection activities and issues. The SCCs are self-organized, self-run, and self-governed, with a spokesperson designated by the sector membership. Specific membership will vary from sector to sector, reflecting the unique composition of each sector; however, membership should be representative of a broad base of owners, operators, associations, and other entities—both large and small—within a sector.

The SCCs enable owners and operators to interact on a wide range of sector-specific strategies, policies, activities, and issues. The SCCs serve as principal sector policy coordination and planning entities. Sectors also rely on ISACs, or other information-sharing mechanisms, which provide operational and tactical capabilities for information sharing and, in some cases, support for incident response activities. (A more detailed discussion of ISAC roles and responsibilities is included in section 4.2.7.)

The primary functions of an SCC include the following:

- Represent a primary point of entry for government into the sector for addressing the entire range of CIKR protection activities and issues for that sector;
- Serve as a strategic communications and coordination mechanism between CIKR owners, operators, and suppliers, and, as appropriate, with the government during emerging threats or response and recovery operations, as determined by the sector;

- Identify, implement, and support the information-sharing capabilities and mechanisms that are most appropriate for the sector. The ISACs may perform this role if so designated by the SCC;
- Participate in planning efforts related to the development, implementation, update, and revision of the SSPs and review of the Sector Annual Reports;
- Facilitate inclusive organization and coordination of the sector's policy development regarding CIKR protection planning and preparedness, exercises and training, public awareness, and associated plan implementation activities and requirements;
- Advise on the integration of Federal, State, local, and regional planning with private sector initiatives; and
- Provide input to the government on sector R&D efforts and requirements.

The SCCs are encouraged to participate in efforts to develop voluntary consensus standards to ensure that sector perspectives are included in standards that affect CIKR protection.⁷

4.1.2.4 Government Coordinating Councils

A GCC is formed as the government counterpart for each SCC to enable interagency and cross-jurisdictional coordination. The GCC comprises representatives from across various levels of government (Federal, State, local, or tribal), as appropriate to the operating landscape of each individual sector. Each GCC is co-chaired by a representative from the designated SSA with responsibility for ensuring appropriate representation on the GCC and providing cross-sector coordination with State, local, and tribal governments. Each GCC is co-chaired by the DHS Assistant Secretary for Infrastructure Protection or his/her designee.

The GCC coordinates strategies, activities, policy, and communications across governmental entities within each sector. The primary functions of a GCC include the following:

- Provide interagency strategic communications and coordination at the sector level through partnership with DHS, the SSA, and other supporting agencies across various levels of government;
- Participate in planning efforts related to the development, implementation, update, and revision of the NIPP and the SSPs;

⁷ Voluntary consensus standards are developed or adopted by voluntary consensus standards bodies, both domestic and international. These organizations plan, develop, establish, or coordinate standards through an agreed-upon procedure that relies on consensus, although not necessarily on unanimity. Federal law encourages Federal participation in these bodies to increase the likelihood that standards meet both public and private sector needs. Examples of other standards that are distinct from voluntary consensus standards include non-consensus standards, industry standards, company standards, or de facto standards developed in the private sector but not in the full consensus process, standards that are unique to government and developed by government for its own uses, and standards mandated by law.

- Coordinate strategic communications and discussion and resolution of issues among government entities within the sector; and
- Coordinate with and support the efforts of the SCC to plan, implement, and execute the Nation’s CIKR protection mission.

4.1.2.5 Regional Consortium Coordinating Council

The RCCC brings together representatives of regional partnerships, groupings, and governance bodies to enable CIKR protection coordination among CIKR partners within and across geographical areas and sectors.

4.1.2.6 Critical Infrastructure Partnership Advisory Council (CIPAC)

CIPAC directly supports the sector partnership model by providing a legal framework that enables members of the SCCs and GCCs to engage in joint CIKR protection-related discussions. CIPAC serves as a forum for government and private sector partners to engage in a broad spectrum of activities, such as:

- Planning, coordination, implementation, and operational issues;
- Implementation of security and preparedness programs;
- Operational activities related to CIKR protection, including incident response and recovery; and
- Development and support of national policies and plans, including the NIPP and the SSPs.

CIPAC membership consists of private sector CIKR owners and operators, or their representative trade or equivalent associations, from the respective sector’s recognized SCC, and representatives of Federal, State, local, and tribal governmental entities (including their representative trade or equivalent associations) that make up the corresponding GCC for each sector. DHS published a Federal Register Notice on March 24, 2006, announcing the establishment of CIPAC as a FACA-exempt body, pursuant to section 871 of the Homeland Security Act.

4.1.3 Regional Coordination and the Partnership Model

Regional partnerships, organizations, and governance bodies enable CIKR protection coordination among CIKR partners within and across certain geographical areas, as well as planning and program implementation aimed at a common hazard or threat environment. These groupings include public-private partnerships that cross jurisdictional,

sector, and international boundaries and take into account dependencies and interdependencies. They are typically self-organizing and self-governing.

Regional organizations, whether interstate or intrastate, vary widely in terms of mission, composition, and functionality. Regardless of the variations, these organizations provide structures at the strategic and/or operational levels that help address cross-sector CIKR planning and protection program implementation. They may also provide enhanced coordination among jurisdictions within a State where CIKR cross multiple jurisdictions and help sectors coordinate with multiple States that rely on a common set of CIKR. In some instances, State Homeland Security Advisors may serve as focal points for regional initiatives and provide linkages between the regional organizations and the sector partnership model. Based on the nature or focus of the regional initiative, these organizations may link into the sector partnership model, as appropriate, through the individual SCCs or GCCs or cross-sector councils, or more broadly through the RCCC.

4.1.4 International CIKR Protection Cooperation

Many CIKR assets, systems, and networks, both physical and cyber, are interconnected with a global infrastructure that has evolved to support modern economies. Each of the CIKR sectors is linked in varying degrees to global energy, transportation systems, telecommunications, cyber, and other infrastructure. This global system creates benefits and efficiencies, but also brings interdependencies, vulnerabilities, and challenges in the context of CIKR protection. The Nation’s safety, security, prosperity, and way of life depend on these “systems of systems,” which must be protected both at home and abroad.

The NIPP strategy for international CIKR protection coordination and cooperation is focused on:

- Instituting effective cooperation with international CIKR partners, as well as high-priority cross-border protection programs. Specific protective actions are developed through the sector planning process and specified in the SSPs and the annual CFI Action Plan;
- Implementing current agreements and instruments that affect CIKR protection;
- Identifying infrastructure located outside the United States that if disrupted or destroyed would lead to loss of life in the United States, or critically affect the Nation’s economic, industrial, or defensive capabilities; and

- Addressing cross-sector and global issues such as cybersecurity and foreign investment.

International CIKR protection activities require coordination with the DOS and appropriate SSAs and must be designed and implemented to benefit the United States and its international partners.

CIKR protection may be affected by foreign investment and ownership of sector assets. This issue is monitored at the Federal level by the CFIUS. The committee provides a forum for assessing the impact of proposed foreign investments on CIKR protection, monitoring to ensure compliance with agreements that result from CFIUS rulings, and supporting executive branch reviews of telecommunications applications to the Federal Communications Commission (FCC) from foreign entities to assess if they pose any national security threat to CIKR (see appendix 1B.4.2).

4.1.4.1 Cooperation With International Partners

DHS, in coordination with the appropriate SSAs, other Federal agencies, and the Department of State (DOS), works with international partners and other entities involved in the international aspects of CIKR protection to exchange experiences, share information, and develop a cooperative environment to materially improve U.S. CIKR protection. DHS, the DOS, and the SSAs work with foreign governments to identify international interdependencies, vulnerabilities, and risk-mitigation strategies, and through international organizations, such as the Group of Eight (G8), NATO, the European Union, the Organization of American States (OAS), and the Organisation for Economic Co-operation and Development (OECD), to enhance CIKR protection. Forums such as the International Maritime Organization (IMO), a specialized agency of the United Nations, cooperate with a host of partners to govern international shipping; develop and maintain a regulatory framework for shipping; address safety and environmental concerns; legal matters and others. The IMO is based in the United Kingdom and has 168 member states.

While the SSAs and owners and operators generally are responsible for developing CIKR protection programs to address risks that arise from or include international sources or considerations, DHS manages specific programs to enhance the cooperation and coordination needed to address the unique challenges and opportunities posed by the international aspects of CIKR protection. The following DHS efforts augment, but do not supersede or replace, the activities and programs of other Federal agencies or other NIPP partners.

- **Critical Foreign Dependencies Initiative:** In accordance with the NIPP, the Federal Government created a comprehensive inventory of infrastructure located outside the

United States that if disrupted or destroyed would lead to loss of life in the United States or critically affect the Nation's economy or national security. In response to this requirement, DHS worked with the DOS to develop the CFDI, a process designed to ensure that the resulting classified National Critical Foreign Dependencies List is inclusive, representative, and leveraged in a coordinated and responsible manner.

- **International Outreach Program:** DHS, in cooperation with the DOS and other Federal agencies, carries out international outreach activities to engage foreign governments and international/multinational organizations to promote a global culture of CIKR protection. These outreach activities enable international cooperation and engage constituencies that often do not traditionally address CIKR protection. This outreach encourages the development and adoption of best practices, training, and other programs designed to improve the protection of U.S. CIKR overseas, as well as the reliability of international CIKR on which this country depends. Other Federal, State, local, tribal, and private sector entities also engage in international outreach that may be related to CIKR risk mitigation in situations where they work directly with their foreign counterparts.
- **The National Exercise Program (NEP):** DHS provides overarching coordination for the NEP to ensure the Nation's readiness to respond in an all-hazards environment and to practice and evaluate the steady-state protection plans and programs put in place by the NIPP. The NEP provides opportunities through exercises for international partners to engage with Federal, State, and local departments and agencies to address cooperation and cross-border issues, including those related to CIKR protection. DHS and other CIKR partners also participate in exercises sponsored by international partners.
- **National Cyber Exercises:** DHS and its partners conduct exercises to identify, test, and improve coordination of the cyber incident response community, including Federal, State, regional, local, tribal, and international governmental entities, as well as private sector corporations and coordinating councils.

Where applicable, DHS encourages the use of PCII protections to safeguard private sector CIKR information when sharing it with international partners. The PCII Program will solicit the submitter's express permission before sharing the submitter's proprietary CIKR information with international partners.

4.1.4.2 Implementing Current Agreements

DHS, the SSAs, and other Federal agencies have entered into agreements with international partners, including bilateral

and multilateral partnerships, with the assistance of the DOS. The key partners involved in existing agreements include:

- **Canada and Mexico:** CIKR interconnectivity between the United States and its immediate neighbors makes the borders virtually transparent. Electricity, natural gas, oil, roads, rail, food, water, minerals, and finished products cross our borders with Canada and Mexico as a routine component of commerce and infrastructure operations. The importance of this trade, and the infrastructure that support it, was highlighted after the terrorist attacks of September 11, 2001, nearly closed both borders. The United States entered into the 2001 Smart Border Declaration with Canada and the 2002 Border Partnership Declaration with Mexico, in part, to address bilateral CIKR issues. In addition, the 2005 Security and Prosperity Partnership of North America (SPP) established a common approach to security to protect North America from external threats, prevent and respond to threats, and further streamline the secure and efficient movement of legitimate, low-risk traffic across the shared borders.
- **United Kingdom:** The United Kingdom is a close ally of the United States that has extensive experience in counterterrorism and CIKR protection. The United Kingdom has developed substantial expertise in law enforcement and intelligence systems, and in the protection of commercial facilities based on its counterterrorism experience. Like the United States, most of the critical infrastructure in the United Kingdom is privately owned. The government of the United Kingdom developed an effective, sophisticated system to manage public-private partnerships. DHS formed a Joint Contact Group (JCG) with the United Kingdom that brings officials into regular, formal contact to discuss and resolve a range of bilateral homeland security issues.
- **The Group of Eight:** Since September 11, 2001, the infrastructure in several G8 countries has been exploited and used to inflict casualties and fear. As a result, G8 partners underscored their determination to combat all forms of terrorism and to strengthen international cooperation. To that end, within the G8 context, the United States spearheaded various CIKR protection initiatives in 2007 and 2008. The first project focused on G8 delegation nation security planning best practices, vulnerability assessment methodologies, and threat assessments for critical energy infrastructure. The second project focused on Chemical Sector infrastructure protection activities, a timely subject given the release of the CFATS in the United States the previous year. These projects have increased the baseline understanding of the measures underway, as well as the CIKR protection capabilities of each G8 member nation. The G8 provides an effective forum for member nations to work together to reduce global risks to CIKR by sharing best practices and methodologies and to understand common threats. Future projects related to critical infrastructure protection within the G8 will address issues related to interdependencies within and across critical infrastructure systems.
- **Asia-Pacific Economic Cooperation (APEC):** This group is responding to the terrorist threat by pursuing several practical counterterrorist initiatives that are intended to prevent the movement of funds, goods, and people involved in terrorist activities, while at the same time ensuring that the legitimate cross-border movement of goods and people is not impeded. APEC established the Counterterrorism Task Force to assist economies in identifying, assessing, and coordinating counterterrorism capacity building. Other APEC measures include the Secure Trade in the APEC Region (STAR) initiative, under which members have developed measures to secure cargo, protect people in transit, strengthen the security of ships and ports, improve airline passenger systems and crew safety, and strengthen border controls.
- **North Atlantic Treaty Organization:** NATO addresses CIKR protection issues through the Senior Civil Emergency Planning Committee, the senior policy and advisory body to the North Atlantic Council on civil emergency planning and disaster relief matters. The committee is responsible for policy direction and coordination of planning boards and committees in the NATO environment. It has developed considerable expertise that applies to CIKR protection and has planning boards and committees covering ocean shipping, inland surface transport, civil aviation, food and agriculture, industrial preparedness, civil communications planning, civil protection, and civil-military medical issues.
- **European Union:** The United States is engaged in a number of CIKR protection activities with the European Union, including those related to advising the European Union on CIKR risk analysis and management, writ large, as well as counter-explosive device activities. The European Commission is in the process of implementing the European Programme for Critical Infrastructure Protection (EPCIP). This program will affect all 27 nations in the European Union, as well as others in the Euro-Zone that elect to participate. EPCIP will initially focus on the Energy and Transport sectors, with expanded focus on the Telecommunications, Financial, and Chemical sectors in coming years. The United States has engaged the EPCIP leadership for the purpose of offering the assistance necessary to support the implementation of the program, with the ultimate goal of enhancing CIKR protection activities across the board. Furthermore, through both IP and the Science and Technology Directorate, DHS works with the Bureau of Diplomatic Security and

the Office of the Coordinator for Counterterrorism at DOS, DOJ, and the FBI to conduct workshops, seminars, and exercises with the European Union on countering terrorist use of explosive devices. These two activities serve as models for U.S. engagement with the European Union on joint CIKR protection activities.

4.1.4.3 Approach to International Cybersecurity

The United States proactively integrates its: intelligence capabilities to protect the country from cyber attack; its diplomatic outreach, advocacy, and operational capabilities to build awareness, preparedness, capacity, and partnerships in the global community; and its law enforcement capabilities to combat cyber crime wherever it originates. The private sector, international industry associations, and companies with global interests and operations also are engaged in addressing cybersecurity internationally. For example, the U.S.-based Information Technology Association of America participates in international cybersecurity conferences and forums, such as the India-based National Association for Software and Service Companies Joint Conference. These efforts require interaction between policy and operations functions to coordinate national and international activity that is mutually supportive around the globe:

- **International Cybersecurity Outreach:** DHS, in cooperation with the DOS, other Federal departments and agencies, and the private sector, engages in multilateral and bilateral discussions to further international computer security awareness and policy development, as well as incident response team information-sharing and capacity-building objectives. DHS engages in bilateral discussions on cybersecurity issues with various international partners, such as India, Italy, Japan, and Norway. DHS also works with international partners in multilateral and regional forums to address cybersecurity and critical infrastructure information protection. For example, the APEC Telecommunications Working Group recently engaged in a capacity-building program to help member countries develop computer emergency response teams. The OAS has approved a framework proposal by its Cyber Security Working Group to create an OAS regional computer incident response contact network for information sharing and capacity building. Multilateral collaboration to build a global culture of security includes participation in the OECD, the G8, and the United Nations. Many of these countries and organizations have developed mechanisms for engaging the private sector in dialogue and program efforts.
- **Collaboration on Cyber Crime:** The U.S. outreach strategy for comprehensive cyber laws and procedures draws on the Council of Europe Convention on Cyber Crime, as well as:

(1) the G8 High-Tech Crime Working Group's principles for fighting cyber crime and protecting critical information infrastructure, (2) the OECD guidelines on information and network security, and (3) the United Nations General Assembly resolutions based on the G8 and OECD efforts. The goal of this outreach strategy is to encourage foreign governments and regional organizations to join the United States in efforts to protect internationally interconnected systems.

- **Collaborative Efforts for Cyber Watch Warning and Incident Response:** The United States works with key allies on cybersecurity policy and operational cooperation. Leveraging pre-existing relationships among Computer Security Incident Response Teams (CSIRTs), DHS has established a preliminary framework for cooperation on cybersecurity policy, watch and warning, and incident response with several other nations. DHS is also participating in the establishment of an International Watch and Warning Network (IWWN) among cybersecurity policy, computer emergency response, and law enforcement participants from 15 countries. The IWWN will provide a mechanism by which the participating countries can share information to build global cyber situational awareness and coordinate incident response.
- **Partnerships to Address Cyber Aspects of CIKR Protection:** The Federal Government leverages existing agreements such as the SPP and the JCG with the United Kingdom to address the Information Technology Sector and cross-cutting cybersecurity as part of CIKR protection. The trilateral SPP builds on existing bilateral agreements between the United States and Canada and the United States and Mexico by providing a forum to address issues on a dual binational basis. In the context of the JCG, DHS established an action plan to address cybersecurity, watch, warning, incident response, and other strategic initiatives.

4.2 Information Sharing: A Network Approach

The effective implementation of the NIPP is predicated on active participation by government and private sector partners in meaningful, multidirectional information sharing. When owners and operators are provided with a comprehensive picture of threats or hazards to CIKR and participate in ongoing multidirectional information flow, their ability to assess risks, make prudent security investments, and develop appropriate resiliency strategies is substantially enhanced. Similarly, when the government is provided with an understanding of private sector information needs, it can adjust its information collection, analysis, synthesis, and dissemination activities accordingly.

The NIPP information-sharing approach constitutes a shift from a strictly hierarchical to a networked model, allowing distribution and access to information both vertically and horizontally, as well as the ability to enable decentralized decisionmaking and actions. The objectives of the network approach are to:

- Enable secure multidirectional information sharing between and across government and industry that focuses, streamlines, and reduces redundant reporting to the greatest extent possible;
- Implement a common set of all-hazards communications, coordination, and information-sharing capabilities for all CIKR partners;
- Provide CIKR partners with a robust communications framework tailored to their specific information-sharing requirements, risk landscape, and protective architecture;
- Provide CIKR partners with a comprehensive common operating picture that includes timely and accurate information about natural hazards, general and specific terrorist threats, incidents and events, impact assessments, and best practices;
- Provide CIKR partners with timely incident reporting and verification of related facts that owners and operators can use with confidence when considering how evolving incidents might affect their risk posture;
- Provide a means for State, local, tribal, territorial, and private sector partners to be integrated, as appropriate, into the intelligence cycle, to include providing input to the development of intelligence requirements;
- Enable the multidirectional flow of information required for CIKR partners to assess risks, conduct risk management activities, invest in security measures, and allocate resources; and
- Protect the integrity and confidentiality of sensitive information.

Within the CIKR community, information sharing is a means to an end. The objective of an effective environment for information sharing is to provide timely and relevant information that partners can use to make decisions and take the necessary actions to manage CIKR risk.

The CIKR Information-Sharing Environment (ISE) supports three levels of decisionmaking and action: (1) strategic planning and investment, (2) situational awareness and preparedness, and (3) operational planning and response. It provides policy, governance, planning, and coordination of information sharing, as well as a forum for identifying the

types of information necessary for partners to make appropriate decisions and take the necessary actions for effective risk management.

Figure 4.2 illustrates the broad concept of the NIPP multidirectional, networked information-sharing approach within the CIKR ISE. This network consists of components that are connected by a national communications platform, the Homeland Security Information Network (HSIN). HSIN is an all-hazards communications system developed by State and local authorities that connects: all 50 States; 5 territories; Washington, DC; and 50 major urban areas. HSIN is one of the key DHS technology tools for strengthening the protection and ensuring the reliable performance of the Nation's critical infrastructure through communication, coordination, and information sharing. It is an Internet-based platform that enables secure, encrypted, unclassified, and for official use only (FOUO) communication between DHS and vetted members within and across CIKR sectors so that partners can obtain, analyze, and share information. The diagram illustrates how this information exchange capability is used for two-way and multidirectional information sharing among: DHS; the Federal Intelligence Community; Federal departments and agencies; State, local, and tribal jurisdictions; and the private sector. The connectivity of the network also allows these partners to share information and coordinate among themselves (e.g., State-to-State coordination). CIKR partners are grouped into nodes in the information-sharing network approach.

4.2.1 Supporting the CIKR Protection Mission

The primary objectives of the NIPP networked approach to information sharing include enhancing situational awareness and maximizing the ability of government and private sector partners at all levels to assess risks and execute risk-mitigation programs and activities. Implementation of the Nation's CIKR protection mission depends on the ability of the government to receive and provide timely, actionable information on emerging threats to CIKR owners and operators and security professionals to support the necessary steps to mitigate risk.

Ongoing and future information-sharing initiatives generally fall within one of four overarching categories:

- **Planning:** All partners have a stake in setting the individual information requirements that best suit the needs of each CIKR sector, driven by the activities in which they need to participate to mitigate CIKR risk. DHS, in conjunction with: the SSAs; SCCs; and other State, local, tribal, territorial, and private sector partners, will collaboratively develop and disseminate an Annual CIKR Protection Information

Requirements Report that summarizes the States and the sectors' input and makes recommendations for information requirements. The Information Requirements Report will be included in the National CIKR Protection Annual Report. In addition to this process, DHS will coordinate with the Intelligence Community to support information collection that reflects the emerging requirements provided by the SSAs and State, local, tribal, territorial, and private sector partners.

- **Information Collection:** Private sector participation in information collection generally is voluntary in nature and includes providing subject matter expertise and operational, vulnerability, and consequence data. Private sector partners also report suspicious activity that could signal pre-operational terrorist activity to the DHS National Operations Center (NOC) through the National Infrastructure Coordinating Center (NICC). Information shared by the private sector, including that which is protected by PCII or other approaches, is integrated into government-collected

information to produce comprehensive threat assessments and threat warning products.

- **Analysis:** HITRAC is responsible for integrating CIKR-specific vulnerability and consequence data with threat information to produce actionable risk assessments used to inform CIKR risk-mitigation activities at all levels. HITRAC analysts work closely with CIKR sector subject matter experts and fusion centers to ensure that these products address the individual requirements of each sector and help actuate corresponding security activities.
- **Dissemination and Decisionmaking:** DHS assessments, such as Site Assistance Visits (SAVs) and Buffer Zone Protection Plans (BZPs), which may include information afforded PCII protection, are shared across the sectors through electronic dissemination, posting to HSIN portals, and direct outreach by DHS. During natural disasters, NISAC provides detailed analyses of the impact of disruptions to CIKR. For

Figure 4-2: NIPP Networked Information-Sharing Approach



example, annually before each hurricane season, NISAC posts to HSIN detailed analyses of impacts to CIKR for areas where hurricane landfall is most likely. Similarly, posted on HSIN are operational cross-sector and sector-specific daily and monthly reports that are culled from open sources. Alerts and notifications of vulnerabilities and incidents are sent to the CIKR sectors and their partners in Federal, State, and local agencies as the necessity arises. These efforts and others provide the private sector with timely, actionable information to enhance situational awareness and enable all-hazards planning activities.

4.2.1.1 Balancing the Sharing and Protection of Information

Effective information sharing relies on the balance between making information available and the ability to protect information that may be sensitive, proprietary, or the disclosure of which might compromise ongoing law enforcement, intelligence, or military operations or methods.

Distribution of information is based on using appropriate protocols for information protection. Whether the sharing is top-down (by partners working with national-level information such as system-wide aggregate data or the results of emergent threat analysis from the Intelligence Community) or bottom-up (by field officers or facility operators sharing detailed and location-specific information), the network approach places shared responsibility on all CIKR partners to maintain appropriate and protected information-sharing practices.

4.2.1.2 Top-Down and Bottom-Up Sharing

During incident situations, DHS monitors risk management activities and CIKR status at the functional/operations level, the local law enforcement level, and the cross-sector level. Information sharing may also incorporate information that comes from pre- and post-event natural disaster warnings and reports. While information sharing is multidirectional within the networked model, there are two primary approaches to information sharing during or in response to a threat or incident.

- **Top-Down Sharing:** Under this approach, information regarding a potential terrorist threat originates at the national level through domestic and/or overseas collection and fused analysis, and is subsequently routed to State and local governments, CIKR owners and operators, and other Federal agencies for immediate attention and/or action. This type of information is generally assessed against DHS analysis reports and integrated with CIKR-related information and data from a variety of government and private sector sources. The result of this integration is the development of

timely information products, often produced within hours, that are available for appropriate dissemination to CIKR partners based on previously specified reporting processes and data formats.

- **Bottom-Up Sharing:** State, local, tribal, private sector, and nongovernmental organizations report a variety of security- and incident-related information from the field using established communications and reporting channels. This bottom-up information is assessed by DHS and its partners in the intelligence and law enforcement communities in the context of threat, vulnerability, consequence, and other information to illustrate a comprehensive risk landscape.

On January 18, 2007, the National Program Manager of the Information Sharing Environment (PM-ISE) and the Federal Information Sharing Council, both established by the Intelligence Reform and Terrorism Prevention Act of 2004, incorporated the CIKR ISE into the national ISE framework. The PM-ISE is seated in the Office of the Director of National Intelligence. Both the National Information Sharing Strategy issued in October 2007 and the Information Sharing Environment Implementation Plan issued in November 2006 recognized that private sector participation in the ISE is composed primarily of CIKR owners and operators, and recognized the role of the NIPP in defining and establishing this portion of the ISE. The PM-ISE designated IP as the Federal Lead for the implementation of the CIKR ISE within the national ISE.

Threat information that is received from local law enforcement or private sector suspicious activity reporting is routed to DHS through the NICC and the NOC. The information is then routed to intelligence and operations personnel to support further analysis or action as required. In the context of evolving threats or incidents, further national-level analyses may result in the development and dissemination of a variety of HITRAC products as discussed in chapter 3. Further information-sharing and incident management activities are based on the results of the integrated national analysis and the needs of key decisionmakers.

DHS also monitors operational information such as changes in local risk management measures, pre- and post-incident disaster or emergency response information, and local law enforcement activities. Monitoring local incidents contributes to a comprehensive picture that supports incident-related damage assessment, recovery prioritization, and other national- or regional-level planning or resource allocation efforts. Written products and reports that result from the

ongoing monitoring are shared with relevant CIKR partners according to appropriate information protection protocols.

4.2.2 The CIKR Information-Sharing Environment

As specified in the Intelligence Reform and Terrorism Prevention Act of 2004, the Federal Government is working with State and local partners and the private sector to create the ISE for terrorism and homeland security information, in which access to such information is matched to the roles, responsibilities, and missions of all organizations engaged in counterterrorism and is timely and relevant to their needs. It is important to note that most of the information shared daily with the CIKR ISE is necessary for coordination and management of risks resulting from natural hazards and accidents. Consequently, for information sharing to be efficient and sustainable for CIKR owners and operators, the same environment needs to be used to share terrorism information.

With its breadth of participants and the complexity of the CIKR protection mission served, CIKR information sharing breaks new ground. It also creates business risks for the owners and operators. Significant questions are raised, such as: What information is required for a productive two-way exchange? How is information most efficiently delivered and to whom to elicit effective action? How is information—both proprietary and government—appropriately protected? How will the sectors take appropriate action in coordination with all levels of government? How can business risks be mitigated when an exchange takes place?

Of particular criticality is the coordination of CIKR information sharing at the national level with that at the local level, where most decisions are made and actions are taken to support the CIKR protection mission. The integration of the CIKR ISE into the national ISE as its private sector component, in recognition of its comprehensiveness and engagement between CIKR owners and operators and all levels of government, strengthens the foundation for effective coordination.

4.2.2.1 CIKR ISE Coordination and Governance

A necessary component for implementing the CIKR ISE is the sector partnership model, which provides the framework for developing requirements for process, policy, technology, levels of performance, and content. It also provides the essential characteristics for defining the “trusted” environment. By using the sector partnership model to develop requirements, the CIKR ISE accommodates a broad range of sector cultures, operations, and risk management approaches and recognizes the unique policy and legal challenges for full two-way sharing of information between the CIKR owners and operators and the various levels of government.

4.2.2.2 Primary Information-Sharing Support Mechanisms

The CIKR ISE encompasses a number of mechanisms that facilitate the flow of information, mitigate obstacles to voluntary information sharing by CIKR owners and operators, and provide feedback and continuous improvement for NIPP information-sharing structures and processes. Other supporting technologies and more traditional methods of communications will continue to support CIKR protection, as appropriate, and will be fully integrated into the network approach.

The Sector Information-Sharing Maturity Model

This capability provides a DHS-supported process to the Sector and Government Coordinating Councils to identify, document, develop, and implement, when needed, core sector-specific and cross-sector coordination and communication business processes among CIKR owners and operators and their government counterparts at all levels. The five core processes for each sector include: alerts, warnings, and notifications; suspicious activity reporting; data management; incident response communication; and routine steady-state collaboration and communication. Defining these business processes in the form of standard operating procedures identifies the necessary participants, clarifies roles and responsibilities, and pre-establishes the necessary and appropriate related actions to be taken by sector and government participants. This capability includes support for the annual testing of these business processes by the sectors to ensure their continued validity and usefulness to their stakeholders.

HSIN

When fully deployed, the HSIN will constitute a robust and significant information-sharing system that supports NIPP-related steady-state CIKR protection and NRF-related incident management activities, as well as serving the information-sharing processes that form the bridge between these two homeland security missions. The linkage between these sets of activities results in a dynamic view of the strategic risk and evolving incident landscape. HSIN functions as one of a number of mechanisms that enable DHS, the SSAs, and other partners to share information. When HSIN is fully developed, users will be able to access ISE terrorism information based on their roles, responsibilities, and missions. The HSIN is composed of multiple, non-hierarchical communities of interest (COIs) that offer CIKR partners the means to share information based on secure access. COIs provide virtual areas where groups of participants with common concerns, such as law enforcement, counterterrorism, critical infrastructure, emergency management, intelligence, international, and other topics, can share information. This structure allows government

and industry partners to engage in collaborative exchanges, based on specific sector-generated information requirements, mission emphasis, or interest level. Within the HSIN-Critical Sectors COI, each sector establishes the rules for participation, including the vetting and verification processes that are appropriate for the sector CIKR landscape and the requirements for information protection. For example, in some sectors, applicants are vetted through the SCC or the ISAC; others may require participants to be documented members of a specific profession, such as law enforcement.

DHS and the SSAs work with other partners to measure the efficacy of the network and to identify areas in which new mechanisms or supporting technologies are needed. The HSIN and the key nodes of the NIPP information-sharing approach are detailed in the following sections. By offering a user-friendly, efficient conduit for information sharing, HSIN enhances the combined effectiveness in an all-hazards environment. HSIN network architecture design is informed by experience gained by DoD and other Federal agencies in developing networks to support similar missions. It supports a secure common operating picture (COP) for all command or watch centers, including those of supporting emergency management and public health activities.

4.2.2.3 Facilitating Usefulness of Information: iCAV and DHS Earth

An important resource that DHS uses to facilitate networked-based information sharing is the iCAV suite of tools and the underlying Geospatial Information Infrastructure (GII). The iCAV and DHS Earth viewers, as well as the GII, provide mechanisms for: industry; Federal, State, and local governments; and other partners to exchange static and real-time information supporting situational and strategic awareness using standards-based information exchange mechanisms. While the iCAV suite of tools permits the viewing of this information in a dynamic map, the GII and IDW provide additional capabilities that allow the data to be shared, stored, and archived in secure, federally compliant standard formats. The iCAV suite of tools also provides the ability to integrate or link a variety of systems and numerous users, ranging from local first-responders to interested agencies within the Federal Government. Through iCAV and DHS Earth, DHS connects previously stove-piped systems, providing consistent, mission-specific COPs across organizational boundaries, fostering horizontal and vertical CIKR information sharing with mission partners.

4.2.3 Federal Intelligence Node

The Federal Intelligence Node, which comprises national Intelligence Community agencies, SSA intelligence offices, and the DHS Office of Intelligence and Analysis (OI&A), identifies and establishes the credibility of general and specific threats. This node also includes national, regional, and field-level information-sharing and intelligence center entities that contribute to information sharing in the context of the CIKR protection mission.

At the national level, these centers include, but are not limited to, the HITRAC, the FBI-led National Joint Terrorism Task Force (NJTTF), the National Counterterrorism Center (NCTC), and the National Maritime Intelligence Center.

- HITRAC analyzes and integrates threat information and works closely with components of the other NIPP information-sharing nodes to generate and disseminate threat warning products and risk analyses to CIKR partners, both internal and external to the network, as appropriate.
- The NJTTF mission is to enhance communications, coordination, and cooperation among Federal, State, local, and tribal agencies representing the intelligence, law enforcement, defense, diplomatic, public safety, and homeland security communities by providing a point of fusion for terrorism intelligence and by supporting Joint Terrorism Task Forces (JTTFs) throughout the United States.
- The NCTC serves as the primary Federal organization for analyzing and integrating all intelligence possessed or acquired by the U.S. Government that pertains to terrorism and counterterrorism, except purely domestic counterterrorism information. The NCTC may, as consistent with applicable law, receive, retain, and disseminate information from any Federal, State, or local government or other source necessary to fulfill its responsibilities.
- The U.S. Coast Guard Intelligence Coordination Center, collocated with the Office of Naval Intelligence at the National Maritime Intelligence Center, serves as the central point of connectivity to fuse, analyze, and disseminate information and intelligence related to the Maritime Transportation System.

At the regional and field levels, Federal information-sharing and intelligence centers include entities such as the local JTTFs, the DHS/DOJ-sponsored Project Seahawk, and FBI Field Intelligence Groups that provide the centralized intelligence/information-sharing component in every FBI field office.

4.2.4 Federal Infrastructure Node

The Federal Infrastructure Node, which comprises DHS, SSAs, GCCs, and other Federal departments and agencies, gathers and receives threat, incident, and other operational information from a variety of sources (including a wide range of watch/operations centers). This information enables assessment of the status of CIKR and facilitates the development and dissemination of appropriate real-time threat and warning products and corresponding protective measures recommendations to CIKR partners (see chapter 3). Participants in the Federal node collaborate with CIKR owners and operators to gain input during the development of threat and warning products and corresponding protective measures recommendations.

4.2.5 State, Local, Tribal, Territorial, and Regional Node

This node provides links among: DHS; the SSAs; and partners at the State, local, tribal, territorial, and regional levels. Several established communications channels provide protocols for passing information from the local to the State to the Federal level and disseminating information from the Federal Government to other partners. The NIPP network approach augments these established communications channels by facilitating two-way and multidirectional information sharing. Members of this node provide incident response, first-responder information, and reports of suspicious activity to the FBI and DHS for the purposes of awareness and analysis. Homeland security advisors receive and further disseminate coordinated DHS/FBI threat and warning products, as appropriate.

Numerous States and urban area jurisdictions also have established fusion centers or terrorism early warning centers to facilitate a collaborative process among law enforcement, public safety, other first-responders, and private entities to collect, integrate, evaluate, analyze, and disseminate criminal intelligence and other information that relates to CIKR protection.

4.2.5.1 State and Local Fusion Centers

Another key mechanism for information exchange at the local level is the SLFCs. SLFCs are developing or integrating operational capabilities that focus on securing CIKR and advancing Federal, State, local, and private sector CIKR protection efforts. These capabilities should incorporate the dissemination of tailored, timely, and actionable analytical products related to CIKR to maximize information sharing and support the risk-reduction activities of the CIKR protection partners. Through such efforts, the capability should be able to support a comprehensive understanding of the threat, local CIKR vulnerabilities, the potential consequences

of attacks, and the effects of risk-mitigation actions not only on risk reduction, but also on business operations within the private sector.

The CIKR functionality described above should be integrated with all other SLFC capabilities to assist fusion centers in achieving their mission. This CIKR functionality should correlate with and complement the baseline capabilities developed for SLFCs. Guidance for SLFCs that support CIKR protection activities is being developed as an appendix to the *Baseline Capabilities for State and Major Urban Area Fusion Centers*. (This document may be obtained at www.it.ojp.gov.) This guidance identifies the additional capabilities that SLFCs should achieve to effectively integrate CIKR protection activities into their analytic and information/intelligence-sharing processes and describes how SLFCs can support risk-reduction efforts taken by Federal, State, local, and private sector partners.

4.2.6 Private Sector Node

The Private Sector Node includes CIKR owners and operators, SCCs, ISACs, and trade associations that provide incident information, as well as reports of suspicious activity that may indicate actual or potential criminal intent or terrorist activity. DHS, in return, provides all-hazards warning products, recommended protective measures, and alert notification to a variety of industry coordination and information-sharing mechanisms, as well as directly to affected CIKR owners and operators.

The NIPP network approach connects and augments existing information-sharing mechanisms, where appropriate, to reach the widest possible population of CIKR owners and operators and other partners. Owners and operators need accurate and timely incident and threat-related information in order to effectively: manage risk; enable post-event response and recovery; and make decisions regarding protection strategies, partnerships, mitigation plans, security measures, and investments for addressing risk.

Information exchange between fusion centers and local partners:

- Site-specific risk information;
- Interdependency information;
- Suspicious activity reports;
- Communications capability information;
- Adversary tactics, techniques, and procedures;
- Best practices;
- Standard operating procedures for incident response; and
- Emergency contact/alert information.

HSPD-7 and the NIPP recognize that CIKR sectors have diverse approaches to establishing their own sectors' information-sharing programs that will most effectively and efficiently meet the requirements of their industry structures, operating cultures, and regulatory regimes. Each sector has the ability to implement a tailored information-sharing solution that may include: privately owned and operated ISACs; voluntary standards development organizations; or other mechanisms, such as trade associations, security organizations, and industry-wide or corporate operations centers, working in concert to expand the flow of knowledge exchange to all infrastructure owners and operators.

ISACs provide an example of a private sector information-sharing and analysis mechanism. Originally recommended by Presidential Decision Directive 63 (PDD-63) in 1998, ISACs are private sector-specific entities that advance physical and cyber CIKR protection by establishing and maintaining collaborative frameworks for operational interaction between and among members and external partners. ISACs, as identified by the sector's SCC, typically serve as the tactical and operational arms for sector information-sharing efforts.

ISAC functions include, but are not limited to: supporting sector-specific information/intelligence requirements for incidents, threats, and vulnerabilities; providing secure capability for members to exchange and share information on cyber, physical, or other threats; establishing and maintaining operational-level dialogue with the appropriate governmental agencies; identifying and disseminating knowledge and best practices; and promoting education and awareness.

ISACs vary greatly in composition (i.e., membership), scope (e.g., focus and coverage within a sector), and capabilities (e.g., 24/7 staffing and analytical capacity), as do the sectors they serve. Most ISACs are members of the ISAC Council, which provides the mechanism for cross-sector sharing of operational information. Sectors that do not have ISACs per se use other mechanisms that participate in the HSIN and other CIKR protection information-sharing arrangements.

4.2.7 DHS Operations Node

The DHS Operations Node maintains close working relationships with other government and private sector partners to enable and coordinate an integrated operational picture, provide operational and situational awareness, and facilitate CIKR information sharing within and across sectors. DHS and other Federal watch/operations centers provide, on a 24/7

basis, the capability required to enable the real-time alerts and warnings, incident reporting, situational awareness, and assessments needed to support CIKR protection.

The principal purpose of a watch/operations center is to collect and share information. Therefore, the value and effectiveness of such centers is largely dependent on a timely, accurate, and extensive population of information sources. The NIPP information-sharing network approach virtually integrates numerous primary watch/operations centers at various levels to enhance information exchange, providing a far-reaching network of awareness and coordination.

4.2.7.1 National Operations Center⁸

The NOC serves as the Nation's hub for domestic incident management operational coordination and situational awareness. The NOC is a standing interagency organization that operates on a 24/7 basis, fusing law enforcement, national intelligence, emergency response, and private sector reporting. The NOC facilitates homeland security information-sharing and operational coordination among Federal, State, local, tribal, and private sector partners, as well as select members of the international community. As such, it is at the center of the NIPP information-sharing network.

The NOC information-sharing and coordination functions include:

- **Information Collection and Analysis:** The NOC maintains national-level situational awareness and provides a centralized, real-time flow of information. An NOC common operating picture is generated using data collected from across the country to provide a broad view of the Nation's current overall risk and preparedness status. Using the common operating picture, NOC personnel, in coordination with the FBI and other agencies, as appropriate, perform initial assessments to gauge the terrorism nexus and track actions taking place across the country in response to a threat, natural disaster, or accident. The information compiled by the NOC is distributed to partners, as appropriate, and is accessible to affected CIKR partners through the HSIN.
- **Situational Awareness and Incident Response Coordination:** The NOC provides the all-hazards information needed to help make decisions and define courses of action.
- **Threat Warning Products:** DHS jointly reviews threat information with the FBI, the Intelligence Community, and other Federal departments and agencies on a continuous basis. When a threat is determined to be credible and

⁸ The Federal Response to Hurricane Katrina: Lessons Learned, issued by the Homeland Security Council, February 2006, recommended the establishment of the NOC as a single entity to unify situational awareness and response, recovery, and mitigation functions. The NOC replaces the DHS Homeland Security Operations Center.

actionable, DHS is responsible for coordinating with these Federal partners in the development and dissemination of threat warning products. This coordination ensures, to the greatest extent possible, the accuracy and timeliness of the information, as well as concurrence by Federal partners.

DHS disseminates threat warning products to Federal, State, local, and tribal governments, as well as to private sector organizations and international partners as COI members through the HSIN, established email distribution lists, and other methods, as required:

- **Threat Advisories:** Contain actionable threat information and provide recommended protective actions based on the nature of the threat. They also may communicate a national, regional, or sector-specific change in the HSAS threat condition.
- **Homeland Security Assessments:** Communicate threat information that does not meet the timeliness, specificity, or criticality criteria of an advisory, but it is pertinent to the security of U.S. CIKR.

The NOC comprises four sub-elements: the NOC Headquarters Element (NOC-HQE), the National Response Coordination Center (NRCC), the intelligence and analysis element, and the NICC:

- **NOC Headquarters Element:** The NOC-HQE is a multi-agency center that provides overall Federal prevention, protection, and preparedness coordination. The NOC-HQE integrates representatives from DHS and other Federal departments and agencies to support steady-state threat-monitoring requirements and situational awareness, as well as operational incident management planning and coordination. The organizational structure of the NOC-HQE is designed to integrate a full spectrum of interagency subject matter expertise, operational planning capability, and reach-back capability to meet the demands of a wide range of potential incident scenarios.
- **National Response Coordination Center:** The NRCC is a multi-agency team operating from FEMA Headquarters that functions as the operational component of the DHS NOC. The NRCC coordinates personnel and resource deployments to support disaster operations and prioritizes inter-agency allocation of resources. It also maintains situational awareness linkages with regional, State, and local partners and a 24/7 watch team.
- **Intelligence and Analysis Element:** The intelligence and analysis element is responsible for interagency intelligence collection requirements, analysis, production, and product dissemination for DHS, to include homeland security threat

warnings, advisory bulletins, and other information pertinent to national incident management (see section 4.2.4).

- **National Infrastructure Coordinating Center:** The NICC, which operates on a 24/7 basis, is a watch/operations center that maintains ongoing operational and situational awareness of the Nation's CIKR sectors. As a CIKR-focused element of the NOC, the NICC provides a centralized mechanism and process for information sharing and coordination among the government, SCCs, GCCs, ISACs, and other industry partners. The NICC receives situational, operational, and incident information from the CIKR sectors in accordance with the information-sharing protocols established in the NRF. The NICC also disseminates products originated by HITRAC that contain all-hazards warning, threat, risk, and CIKR protection information:
 - *Alerts and Warnings:* The NICC disseminates threat-related and other all-hazards information products to an extensive customer base of private sector partners.
 - *Suspicious Activity and Potential Threat Reporting:* The NICC receives and processes reports from the private sector on suspicious activities or potential threats to the Nation's CIKR. The NICC documents the information provided, compiles additional details surrounding the suspicious activity or potential threat, and forwards the report to DHS sector specialists, the NOC, HITRAC, and the FBI.
 - *Incidents and Events:* When an incident or event occurs, the NICC coordinates with DHS sector specialists, industry partners, and other established information-sharing mechanisms to communicate pertinent information. As needed, the NICC generates reports detailing the incident, as well as the sector impacts (or potential impacts), and disseminates them to the NOC.

During Hurricanes Gustav and Ike in 2008, the NICC facilitated critical incident-related information sharing between the government and CIKR owners and operators. Through the Infrastructure Protection Executive Notification Service (ENS), the NICC provided situation reports to the SSAs, which, in turn, contacted their respective CIKR owners and operators and related government agencies to develop impact assessments. Throughout both hurricanes, the SSAs submitted reports twice daily via a secure Web site. These reports included information on damage assessments, restoration activities, and key issues or concerns. The NICC compiled the SSA reports and uploaded the CIKR portion of the DHS Situation Report into the COP and/or HSIN-CS for access by the SSAs and CIKR owners and operators.

- *National Response Planning and Execution*: The NICC supports the NRF by facilitating information sharing among the SCCs, GCCs, ISACs, and other partners during CIKR mitigation, response, and recovery activities.

4.2.7.2 National Coordinating Center for Telecommunications

Pursuant to Executive Order 12472, the National Communications System (NCS) assists the President, National Security Council, Homeland Security Council, Office of Science and Technology Policy (OSTP), and OMB in the coordination and provision of NS/EP communications for the Federal Government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution. As called for in the Executive Order, the NCS has established the National Coordinating Center for Telecommunications (NCC), which is a joint industry-government entity. Under the Executive Order, the NCC assists the NCS in the initiation, coordination, and recovery of NS/EP communications services or facilities under all conditions of crisis or emergency. The NCC regularly monitors the status of communications systems. It collects situational and operational information on a regular basis, as well as during a crisis, and provides information to the NCS. The NCS, in turn, shares information with the White House and other DHS components.

4.2.7.3 United States Computer Emergency Readiness Team

The United States Computer Emergency Readiness Team (US-CERT), which operates on a 24/7 basis, is a single point of contact for cyberspace analysis, warning, information sharing, and incident response and recovery for CIKR partners. It is a partnership between DHS and the public and private sectors designed to enable protection of cyber infrastructure and to coordinate the prevention of and response to cyber attacks across the Nation.

US-CERT coordinates with CIKR partners to disseminate reasoned and actionable cybersecurity information through a Web site, accessible through the HSIN, and through mailing lists. Among the products that it provides are:

- **Cybersecurity Bulletins**: Weekly bulletins written for systems administrators and other technical users that summarize published information concerning new security issues and vulnerabilities.
- **Technical Cybersecurity Alerts**: Written for system administrators and experienced users, technical alerts provide timely information on current security issues, vulnerabilities, and exploits.
- **Cybersecurity Alerts**: Written in a language for home, corporate, and new users, these alerts are published in conjunction with technical alerts when there are security issues that affect the general public.
- **Cybersecurity Tips**: Tips provide information and advice on a variety of common security topics. They are published biweekly and are primarily intended for home, corporate, and new users.
- **National Web Cast Initiative**: DHS, through US-CERT and the Multi-State Information Sharing and Analysis Center (MS-ISAC), has initiated a joint partnership to develop a series of national Web casts that will examine critical and timely cybersecurity issues. The purpose of the initiative is to strengthen the Nation's cyber readiness and resilience.

US-CERT also provides a method for citizens, businesses, and other important institutions to communicate and coordinate directly with the Federal Government on matters of cybersecurity. The private sector can use the protections afforded by the Critical Infrastructure Information Act to electronically submit proprietary data to US-CERT.

4.2.8 Other Information-Sharing Nodes

DHS, other Federal agencies, and the law enforcement community provide additional services and programs that share information supporting CIKR protection with a broad range of partners. These include, but are not limited to, the following:

- **Sharing National Security Information**: DHS sponsors security clearances for designated private sector owners and operators to promote the sharing of classified information using currently available methods and systems.
- **FBI Law Enforcement Online (LEO)**: LEO can be accessed by any approved employee of a Federal, State, or local law enforcement agency, or approved member of an authorized law enforcement special interest group. LEO provides a communications mechanism to link all levels of law enforcement throughout the United States.
- **RISSNET™** is a secure nationwide law enforcement and information-sharing network that operates as part of the Regional Information Sharing Systems (RISS) Program. RISS is composed of six regional centers that share intelligence and coordinate efforts targeted against criminal networks, terrorism, cyber crime, and other unlawful activities that cross jurisdictional lines. RISSNET features include online access to a RISS electronic bulletin board, databases, RISS center Web pages, secure email, a RISS search engine, and other center resources. The RISS program is federally funded and administered by the DOJ/Bureau of Justice Assistance.

- **FBI InfraGard:** InfraGard is a partnership among the FBI, other governmental entities, and the private sector. The InfraGard National Membership Alliance is an association of businesses, academic institutions, State and local law enforcement agencies, and other participants that enables the sharing of knowledge, expertise, information, and intelligence related to the protection of U.S. CIKR from physical and cyber threats.
- **The United States Coast Guard (USCG) HOMEPORT:** The HOMEPORT Web site is an Internet-enabled venue capable of supporting the sharing of sensitive information among Federal, State, local, and private sector maritime regulatory or security personnel. HOMEPORT is the primary means of informing members of local Maritime Security Committees.
- **Interagency Cybersecurity Efforts:** The intelligence and law enforcement communities have various information-sharing mechanisms in place. Examples include:
 - *U.S. Secret Service Electronic Crimes Task Forces (ECTFs):* ECTFs prevent, detect, and investigate electronic crimes, cyber-based attacks, and intrusions against CIKR and electronic payment systems, and provide interagency information sharing on related issues.
 - *Cybercop Portal:* The DHS-sponsored Cybercop portal is a secure Internet-based information-sharing mechanism that connects more than 5,300 members of the law enforcement community, bank investigators, and the network security specialists involved in electronic crimes investigations.

4.3 Protection of Sensitive CIKR Information

NIPP implementation will rely greatly on critical infrastructure information provided by the private sector and State and local governments. Much of this is sensitive business or security information that could cause serious damage to companies, the economy, and public safety or security through unauthorized disclosure or access to this information.

The Federal Government has a statutory responsibility to safeguard information collected from or about CIKR activities. Section 201(d)(12)(a) of the Homeland Security Act requires DHS to “ensure that any material received pursuant to this Act is protected from unauthorized disclosure and handled and used only for the performance of official duties.” DHS and other Federal agencies use a number of programs and procedures, such as the PCII Program, to ensure that CIKR information is properly safeguarded. In addition to the PCII Program, other programs and procedures used to protect sensitive information include Sensitive Security Information

for transportation activities, Unclassified Controlled Nuclear Information (UCNI), Safeguards Information, contractual provisions, classified national provisions, Classified National Security Information, Law Enforcement Sensitive Information, Federal Security Information Guidelines, Federal Security Classification Guidelines, and other requirements established by law.

4.3.1 Protected Critical Infrastructure Information Program

The PCII Program was established pursuant to the Critical Infrastructure Information (CII) Act of 2002. The program institutes a means for the voluntary sharing of private sector, State, and local CIKR information with the Federal Government while providing assurances that the information will be exempt from public disclosure and will be properly safeguarded.

The PCII Program, which operates under the authority of the CII Act and the implementing regulation (6 Code of Federal Regulations (CFR) Part 29 (the Final Rule)), defines both the requirements for submitting CII and those that governmental entities must meet for accessing and safeguarding PCII. DHS remains committed to making PCII an effective tool for robust information sharing between critical infrastructure owners and operators and the government. For more information, contact the PCII Program Office at pcii-info@dhs.gov. Additional PCII Program information may also be found at www.dhs.gov/pcii.

4.3.1.1 PCII Program Office

The PCII Program Office is responsible for managing PCII Program requirements, developing protocols for handling PCII, raising awareness of the need for protected information sharing between different levels of government and the private sector, and ensuring that programs receiving voluntary CII submissions that have been validated as PCII use approved procedures to continuously safeguard submitted information. The Program Office collaborates with governmental organizations and the private sector to develop information-sharing partnerships that promote greater homeland security.

4.3.1.2 Critical Infrastructure Information Protection

The following processes and procedures apply to all CII submissions:

- Individuals or collaborative groups may submit information for protection to either the PCII Program Office or a Federal PCII Program Manager Designee;
- The PCII Program Office validates the information as PCII if it qualifies for protection under the CII Act;

- All PCII is stored in secure data management systems and CIKR partners follow PCII Program safeguarding, handling, dissemination, and storage requirements established in the Final Rule and promulgated by the PCII Program Office;
- Secure methods are used for disseminating PCII, which may only be accessed by authorized PCII users who have taken the PCII Program training (see section 6.2 for PCII training offerings), have homeland security duties, and have a need to know for the specific PCII;
- Authorized users must comply with the safeguarding requirements defined by the PCII Program Office; and
- Any suspected disclosure of PCII will be promptly investigated.

The Final Rule invested the PCII Program Manager with the authority and flexibility to designate certain types of CII as presumptively valid PCII to accelerate the validation process and to facilitate submissions directly to the SSAs and other Federal partners. This is known as a “categorical inclusion.” Specifically, categorical inclusions allow:

- The PCII Program Manager to establish categories of information for which PCII status will automatically apply;
- Indirect submissions to DHS through DHS field representatives and other Federal partners; and
- The PCII Program Office to designate DHS field representatives and Federal partners other than DHS to receive CII indirectly on behalf of DHS, but only the PCII Program Manager is authorized to make the decision to validate a submission as PCII.

The Final Rule enables submitters to submit their CII directly to a PCII Program Manager Designee within a given Federal agency. Interested submitters should contact the PCII Program Office at pcii-info@dhs.gov to determine whether a Federal partner has an appropriate PCII categorical inclusion program established. If not, the PCII Program Office will work with the submitter and the relevant Federal partner to establish a program and facilitate the application of PCII protections to the submitter’s CIKR information.

4.3.1.3 Uses of PCII

PCII may be shared with accredited governmental entities, including authorized Federal, State, or local government employees or contractors supporting Federal agencies, only for the purposes of securing CIKR and protected systems. PCII will be used for analysis, prevention, response, and recovery of CIKR threatened by terrorism or other hazards.

PCII may be used to generate advisories, alerts, and warnings relevant to the private sector. Communications available to the public, however, will not contain any actual PCII. PCII can be combined with other information, including classified information to support CIKR protection activities, but must be marked accordingly.

The CII Act specifically authorizes disclosure of PCII without the permission of the submitter to:

- Further an investigation or prosecute a criminal act;
- Either House of Congress, to the extent that they address matters within their jurisdiction, or any related committee, subcommittee, or joint committee; and
- The Comptroller General or any authorized representative of the Comptroller General, while performing the duties of the Government Accountability Office.

4.3.1.4 PCII Protections and Authorized Users

The PCII Program has established policies and procedures to ensure that PCII is properly accessed, used, and safeguarded throughout its life cycle. These safeguards ensure that submitted information is:

- Used appropriately for homeland security purposes;
- Accessed only by authorized and properly trained government employees and contractors with homeland security duties who have a need to know and for non-Federal government employees who have signed a Non-Disclosure Agreement;
- Protected from disclosure under the Freedom of Information Act (FOIA) and similar State and local disclosure laws, and from use in civil litigation and regulatory actions; and
- Protected and handled in a secure manner.

The law and rule prescribe criminal penalties for intentional unauthorized access, distribution, and misuse of PCII, including the following provisions:

- Federal employees may be subject to disciplinary action, including criminal and civil penalties and loss of employment;
- Contract employees may face termination and the contractor may have its contract terminated; and
- The CII Act sanctions for unauthorized disclosure of PCII apply only to Federal personnel. In order to become accredited, State and local participating entities must demonstrate that they can apply appropriate State and local penalties for improperly handling sensitive information such as PCII.

PCII is actively used by numerous DHS information collection and assessment tools, including the C/ACAMS, BZPs, and SAVs. PCII also partners with many Federal agencies, notably the Department of Health and Human Services (HHS) and DoD. In addition, the PCII Program actively partners with all State, local, and territorial governments interested in accessing PCII.

4.3.2 Other Information Protection Protocols

Information protection protocols may impose requirements for access or other standard processes for safeguarding information. Information need not be validated as PCII to receive security protection and disclosure restrictions. Several categories of information related to CIKR are considered to be sensitive and require protection, but are not classified. The major categories that currently apply to CIKR are discussed below.

4.3.2.1 Sensitive Security Information (SSI)

The Maritime Transportation Security Act, the Aviation Transportation Security Act, and the Homeland Security Act establish protection for Sensitive Security Information (SSI). The Transportation Security Administration (TSA) and the USCG may designate information as SSI when disclosure would:

- Be detrimental to security;
- Reveal trade secrets or privileged or confidential information; or
- Constitute an unwarranted invasion of privacy.

Parties accessing SSI must demonstrate a need to know. Holders of SSI must protect such information from unauthorized disclosure and must destroy the information when it is no longer needed. SSI protection pertains to government officials, as well as to Transportation Systems Sector owners and operators.

4.3.2.2 Unclassified Controlled Nuclear Information (UCNI)

DoD and DOE may designate certain information as UCNI. Such information relates to the production, processing, or use of nuclear material; nuclear facility design information; and security plans and measures for the physical protection of nuclear materials. This designation is used when disclosure could affect public health and safety or national security by enabling illegal production or diversion of nuclear materials or weapons. Access to UCNI is restricted to those who have a need to know. Procedures are specified for marking and safeguarding UCNI.

4.3.2.3 Safeguards Information (SGI)

Safeguards Information (SGI) is a special category of sensitive unclassified information authorized by Section 147 of the Atomic Energy Act of 1954, as amended. SGI concerns the physical protection of operating power reactors, spent fuel shipments, strategic special nuclear material, or other radioactive material. While SGI is considered sensitive unclassified information, its handling and protection more closely resemble the handling of classified Confidential information than other sensitive unclassified information. The categories of individuals who are permitted access to SGI and the access requirements are listed in 10 CFR 73.21.

4.3.2.4 Freedom of Information Act Exemptions and Exclusions

FOIA was enacted in 1966 and amended and modified by congressional legislation, including the Privacy Act of 1974, the Electronic Freedom of Information Act of 1996, and the OPEN Government Act of 2007. The act established a statutory right of public access to executive branch information in the Federal Government and generally provides that any person has a right, enforceable in court, to obtain access to Federal agency records. Certain records may be protected from public disclosure under the act if they fall into one of three special law enforcement exclusions that protect information, such as informants' names. They may also be protected from public disclosure under the act if they are in one of nine exemption categories that protect such information as classified national security data, personnel and medical files, information that Congress exempted by another statute, trade secrets or financial information obtained by the government from individuals, information subject to common law privileges, certain law enforcement records, and information exempt on privacy grounds.

4.3.2.5 Classified Information

Under amended Executive Orders 12958 and 12829, the Information Security Oversight Office of the National Archives is responsible to the President for overseeing the security classification programs in both government and industry that safeguard National Security Information (NSI), including information related to defense against transnational terrorism.

Specific characteristics distinguish classified information from other sensitive information. These include:

- Information can only be designated as classified by a duly empowered authority;
- Information classified by one classification authority must be handled by others in accordance with the guidelines issued by the classifying authority;

- Information must be owned by, produced by or for, or under the control of the Federal Government;
- Unauthorized disclosure of the information could reasonably be expected to result in damage to U.S. national security; and
- The information falls into one or more of the categories of information listed below:
 - Military plans, weapons systems, or operations;
 - Foreign government information;
 - Intelligence activities (including special activities), intelligence sources or methods, or cryptology;
 - Foreign relations or foreign activities of the United States, including confidential sources;
 - Scientific, technological, or economic matters related to national security, which includes defense against transnational terrorism;
 - Federal Government programs for safeguarding nuclear materials or facilities;
 - Vulnerabilities or capabilities of systems, installations, infrastructure, projects, plans, or protection services related to national security, which includes defense against transnational terrorism; or
 - Weapons of mass destruction.

Many forms of information related to CIKR protection have these characteristics. This information may be determined to be classified information and must be protected accordingly.

4.3.2.6 Physical Security and Cybersecurity Measures

DHS uses strict information security protocols for the access, use, and storage of sensitive information, including that related to CIKR. These protocols include both physical security measures and cybersecurity measures. Physical security protocols for DHS facilities require access control and risk-mitigation measures. Information security protocols include access controls, login restrictions, session tracking, and data labeling. Appendix 3C provides a discussion of these protections as applied to the IDW.

4.3.2.7 Chemical-Terrorism Vulnerability Information

On April 9, 2007, DHS issued the CFATS. Congress authorized these interim final regulations (IFR) under section 550 of the Department of Homeland Security Appropriations Act of 2007, directing the department to identify, assess, and ensure effective security at high-risk chemical facilities. In section 550,

Congress also acknowledged DHS's need to both protect and share chemical facility security information with appropriate third parties. Consequently, DHS included provisions in the IFR to create and explain Chemical-Terrorism Vulnerability Information (CVI), a new category of protected information to protect extremely sensitive information that facilities develop for the purposes of complying with the CFATS, which could be exploited by terrorists. At the same time, CVI allows the sharing of relevant information with State and local government officials who have a need to know CVI in order to carry out chemical facility security activities. Before being authorized to access CVI, individuals will have to complete training to ensure that they understand and comply with the various safeguarding and handling requirements for CVI.

More information on CFATS and CVI, including the CVI Procedures Manual, can be found at www.dhs.gov/chemicalsecurity.

4.4 Privacy and Constitutional Freedoms

Mechanisms detailed in the NIPP are designed to obtain a high level of security while protecting the privacy, civil rights, and civil liberties that form an integral part of America's national character. In providing for effective protection programs, the processes outlined in the NIPP respect privacy, freedom of expression, freedom of movement, freedom from unlawful discrimination, and other liberties that define the American way of life. Compliance with the Privacy Act and governmental privacy regulations and procedures is a key factor that is considered when collecting, maintaining, using, and disseminating personally identifiable information. The following DHS offices support the NIPP processes:

- **DHS Privacy Office:** Pursuant to Section 222 the Homeland Security Act, DHS has designated a Chief Privacy Officer to establish privacy policy within the Department and to work with programs and offices to ensure their compliance with all applicable privacy laws and policies. The DHS Privacy Office conducts privacy impact assessments which identify potential privacy risks, details steps programs have taken to mitigate those potential risks, and makes recommendations that programs may implement to further reduce risks to privacy. The DHS Chief Privacy Officer, moreover consults regularly with privacy advocates, industry experts, and the public at large to provide transparency and ensure broad input and consideration of privacy issues, so that DHS achieves solutions that protect privacy while enhancing security.

- **DHS Office for Civil Rights and Civil Liberties:** Pursuant to the Homeland Security Act, the Office for Civil Rights and Civil Liberties provides legal and policy advice to department leadership on civil rights and civil liberties issues to ensure our freedoms are preserved while protecting the homeland. The Office for Civil Rights and Civil Liberties also investigates and resolves complaints from the public concerning civil rights and civil liberties abuses or racial, ethnic, or religious profiling.

5. CIKR Protection as Part of the Homeland Security Mission

This chapter describes the linkages between the NIPP, the SSPs, and other CIKR protection strategies, plans, and initiatives that are most relevant to the overarching national homeland security and CIKR protection missions. It also describes how the unified national CIKR protection effort integrates elements of the homeland security mission, including preparedness and activities to prevent, protect against, respond to, and recover from terrorist attacks, major disasters, and other emergencies. Sector-specific linkages to these other national frameworks are addressed in the SSPs.

5.1 A Coordinated National Approach to the Homeland Security Mission

The NIPP provides the structure needed to coordinate, integrate, and synchronize activities derived from various relevant statutes, national strategies, and Presidential directives to create a unified national approach to implementing the CIKR protection mission. The relevant authorities include those that address the overarching homeland security and CIKR protection missions, as well as those that address a wide range of sector-specific CIKR protection-related functions, programs, and responsibilities. This section describes how overarching homeland security legislation, strategies, HSPDs, and related initiatives work together (see figure 5-1). Information regarding sector-specific CIKR-related authorities is addressed in the respective SSPs.

5.1.1 Legislation

The Homeland Security Act of 2002 (figure 5-1, column 1) provides the primary authority for the overall homeland security mission and establishes the basis for the NIPP, the SSPs, and related CIKR protection efforts and activities. A number of other statutes (as described in chapter 2 and

appendix 2A) provide authorities for cross-sector and sector-specific CIKR protection activities. Individual SSPs address relevant sector-specific authorities.

Public Law 110-53, Implementing Recommendations of the 9/11 Commission Act of 2007, further refines and enumerates the authorities specified in the Homeland Security Act and formally assigns key infrastructure protection responsibilities to DHS, including the creation of a database of all national infrastructure to support cross-sector risk assessment and management.

5.1.2 Strategies

The National Strategy for Homeland Security, The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, and The National Strategy to Secure Cyberspace together provide the vision and strategic direction for the CIKR protection elements of the homeland security mission (see figure 5-1, column 1). A number of other Presidential strategies, such as the National Intelligence Strategy, provide direction and guidance related to CIKR protection on a national or sector-specific basis (see appendix 2A).

5.1.2.1 The National Strategy for Homeland Security

The President’s National Strategy for Homeland Security (2002) established protection of America’s CIKR as a core homeland security mission and as a key element of the comprehensive approach to homeland security and domestic incident management. This strategy articulated the vision for a unified “American Infrastructure Protection effort” to “ensure we address vulnerabilities that involve more than one infrastructure sector or require action by more than one agency” and to “assess threats and vulnerabilities comprehensively across all infrastructure sectors to ensure we reduce the overall risk to the country, instead of inadvertently shifting risk from one potential set of targets to another.”

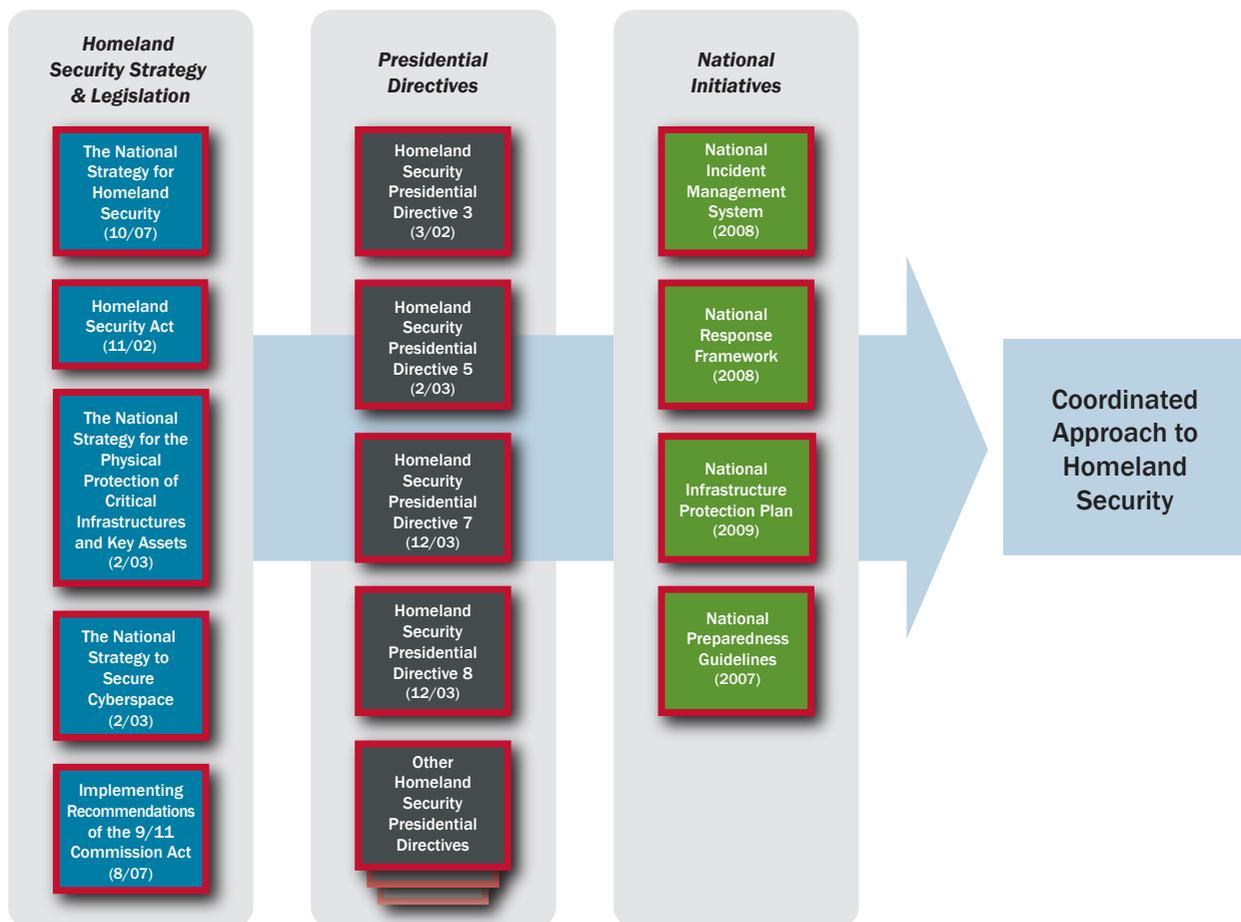
This strategy called for the development of “interconnected and complementary homeland security systems that are reinforcing rather than duplicative, and that ensure essential requirements are met ... [and] provide a framework to align the resources of the Federal budget directly to the task of securing the homeland.”

The 2007 National Strategy for Homeland Security builds on the first National Strategy for Homeland Security and complements both the National Security Strategy issued in March 2006 and the National Strategy for Combating Terrorism issued in September 2006. It reflects the increased understanding of threats confronting the United States, incorporates lessons learned from exercises and real-world catastrophes, and addresses ways to ensure long-term success by strengthening the homeland security foundation that has been built.

5.1.2.2 The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets identifies national policy, goals, objectives, and principles needed to “secure the infrastructures and assets vital to national security, governance, public health and safety, economy, and public confidence.” The strategy: identifies specific initiatives to drive near-term national protection priorities and inform the resource allocation process;

Figure 5-1: National Framework for Homeland Security



identifies key initiatives needed to secure each of the CIKR sectors; and addresses specific cross-sector security priorities. Additionally, it establishes a foundation for building and fostering the cooperative environment in which government, industry, and private citizens can carry out their respective protection responsibilities more effectively and efficiently.

5.1.2.3 The National Strategy to Secure Cyberspace

The National Strategy to Secure Cyberspace sets forth objectives and specific actions needed to prevent cyber attacks against America's CIKR, identifies and appropriately responds to those responsible for cyber attacks, reduces nationally identified vulnerabilities, and minimizes damage and recovery time from cyber attacks. This strategy articulates five national priorities, including the establishment of a security response system, a threat and vulnerability reduction program, awareness and training programs, efforts to secure government cyberspace, and international cooperation.

Priority in this strategy is focused on improving the national response to cyber incidents, reducing threats from and vulnerabilities to cyber attacks, preventing cyber attacks that could affect national security assets, and improving the international management of and response to such attacks.

5.1.2.4 Implementing Recommendations of the 9/11 Commission Act of 2007

This act requires the implementation of some of the recommendations made by the 9/11 Commission, to include requiring the Secretary of Homeland Security to: (1) establish department-wide procedures to receive and analyze intelligence from State, local, and tribal governments and the private sector; and (2) establish a system that screens 100 percent of maritime and passenger cargo. The act also established grants to support high-risk urban areas and State, local, and tribal governments in preventing, preparing for, protecting against, and responding to acts of terrorism, and to assist States in carrying out initiatives to improve international emergency communications.

Title IX of the act requires DHS to establish a common set of criteria for private sector preparedness in disaster management, emergency management, and business continuity. These Voluntary Private Sector Preparedness Standards will be accredited and certified by the American National Standards Institute (ANSI) and the American Society for Quality (ASQ) National Accreditation Board (ANAB).

The act also established grants to support high-risk urban areas and State, local, and tribal governments in preventing, preparing for, protecting against, and responding to acts of terrorism.

5.1.3 Homeland Security Presidential Directives and National Initiatives

Homeland Security Presidential Directives set national policies and executive mandates for specific programs and activities (see figure 5-1, column 2). The first was issued on October 29, 2001, shortly after the attacks on September 11, 2001, establishing the Homeland Security Council. It was followed by a series of directives regarding the full spectrum of actions required to "prevent terrorist attacks within the United States; reduce America's vulnerability to terrorism, major disasters, and other emergencies; and minimize the damage and recover from incidents that do occur." A number of these are relevant to CIKR protection. HSPD-3, Homeland Security Advisory System, provides the requirement for the dissemination of information regarding terrorist acts to Federal, State, and local authorities, and the American people. HSPD-5 addresses the national approach to domestic incident management; HSPD-7 focuses on the CIKR protection mission; and HSPD-8 focuses on ensuring the optimal level of preparedness to protect, prevent, respond to, and recover from terrorist attacks and the full range of natural and man-made hazards.

This section addresses the Homeland Security Presidential Directives that are most relevant to the overarching CIKR protection component of the homeland security mission (e.g., HSPD-3, -5, -7, and -8). Other related Presidential directives, such as: HSPD-9, Defense of the United States Agriculture and Food; HSPD-10, Biodefense for the 21st Century; and HSPD-22, Domestic Chemical Defense, are relevant to CIKR protection in specific sectors and are addressed in further detail in the appropriate SSPs. Additional HSPDs are also described in appendix 2A.

5.1.3.1 HSPD-3, Homeland Security Advisory System

HSPD-3 (March 2002) established the policy for the creation of the HSAS to provide warnings to Federal, State, and local authorities, and the American people in the form of a set of graduated threat conditions that escalate as the risk of the threat increases. At each threat level, Federal departments and agencies are required to implement a corresponding set of protective measures to further reduce vulnerability or increase response capabilities during a period of heightened alert. The threat conditions also serve as guideposts for the implementation of tailored protective measures by State, local, tribal, and private sector partners.

5.1.3.2 HSPD-5, Management of Domestic Incidents

HSPD-5 (February 2003) required DHS to lead a coordinated national effort with: other Federal departments and agencies;

State, local, and tribal governments; and the private sector to develop and implement NIMS and the NRF (see figure 5-1, column 4).

The NIMS (December 2008) provides a nationwide template enabling: Federal, State, local, and tribal governments; the private sector; and nongovernmental organizations to work together effectively and efficiently to prevent, protect against, respond to, and recover from incidents regardless of cause, size, and complexity. The NIMS provides a uniform doctrine for command and management, including: Incident Command, Multi-Agency Coordination, and Joint Information Systems; resource, communications, and information management; and application of supporting technologies.

The NRP (December 2004) was superseded by the National Response Framework (January 2008). Both the NRP and the NRF were built on the NIMS template to establish a single, comprehensive framework for the management of domestic incidents (including threats) that require DHS coordination and effective response and engaged partnership by an appropriate combination of: Federal, State, local, and tribal governments; the private sector; and nongovernmental organizations. The NRF includes a CIKR Support Annex that provides the policies and protocols for integrating the CIKR protection mission as an essential element of domestic incident management and establishes the Infrastructure Liaison function to serve as a focal point for CIKR coordination at the field level.

5.1.3.3 HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection

HSPD-7 (December 2003) established the U.S. policy for “enhancing protection of the Nation’s CIKR.” It mandated development of the NIPP as the primary vehicle for implementing the CIKR protection policy. HSPD-7 directed the Secretary of Homeland Security to lead development of the plan, including, but not limited to, the following four key elements:

- A strategy to identify and coordinate the protection of CIKR;
- A summary of activities to be undertaken to prioritize, reduce the vulnerability of, and coordinate protection of CIKR;
- A summary of initiatives for sharing information and for providing threat and warning data to State, local, and tribal governments, and the private sector; and
- Coordination and integration, as appropriate, with other Federal emergency management and preparedness activities, including the NRF and guidance provided in the National Preparedness Guidelines.

HSPD-7 also directed the Secretary of Homeland Security to maintain an organization to serve as a focal point for the security of cyberspace. The NIPP is supported by a series of SSPs, developed by the SSAs in coordination with their public and private sector partners, which detail the approach to CIKR protection goals, initiatives, processes, and requirements for each sector.

5.1.3.4 HSPD-8, National Preparedness

HSPD-8 (December 2003) mandates the development of a national preparedness goal, which was finalized in the National Preparedness Guidelines (see figure 5-1, column 3), aimed at helping entities at all levels of government build and maintain the capabilities to prevent, protect against, respond to, and recover from major events “to minimize the impact on lives, property, and the economy.”

To do this, the National Preparedness Guidelines provide readiness targets, priorities, standards for assessments and strategies, and a system for assessing the Nation’s overall level of preparedness across four mission areas: prevention, protection, response, and recovery. There are four critical elements of the National Preparedness Guidelines:

- **The National Preparedness Vision**, which provides a concise statement of the core preparedness goal for the Nation.
- **The National Planning Scenarios**, which depict a diverse set of high-consequence threat scenarios of both potential terrorist attacks and natural disasters. Collectively, the 15 scenarios are designed to focus contingency planning for homeland security preparedness work at all levels of government and with the private sector. The scenarios form the basis for coordinated Federal planning, training, exercises, and grant investments needed to prepare for emergencies of all types.
- **The Universal Task List (UTL)**, which is a menu of some 1,600 unique tasks that can facilitate efforts to prevent, protect against, respond to, and recover from the major events that are represented by the National Planning Scenarios. It presents a common vocabulary and identifies key tasks that support the development of essential capabilities among organizations at all levels. No entity is expected to perform every task.
- **The Target Capabilities List (TCL)**, which defines 37 specific capabilities that communities, the private sector, and all levels of government should collectively possess in order to respond effectively to disasters.

The National Preparedness Guidelines use capabilities-based planning processes and enable Federal, State, local, and

tribal entities to prioritize needs, update strategies, allocate resources, and deliver programs. The guidelines reference standard planning tools that are applicable to the implementation of the NIPP, including the UTL and the TCL. Like the NIPP, the UTL and TCL are living documents that will be enhanced and refined over time.

Annex 1 (December 2007) to HSPD-8 established a standard and comprehensive approach to national planning intended to enhance the preparedness of the Nation. The annex articulated the U.S. Government policy “to integrate effective policy and operational objectives to prevent, protect against, respond to, and recover from all hazards, and comprises: (a) a standardized Federal planning process; (b) national planning doctrine; (c) resourced operational and tactical capabilities at each Federal department and agency with a role in homeland security; (d) strategic guidance, strategic plans, concepts of operations, and operations plans and, as appropriate, tactical plans; and (e) a system for integrating plans among all levels of government.”

5.1.3.5 HSPD-19, Combating Terrorist Use of Explosives in the United States

In February 2007, the President signed HSPD-19, Combating Terrorist Use of Explosives in the United States, requiring the Attorney General to develop a report for the President, including a national strategy and recommendations, on how to more effectively deter, prevent, detect, protect against, and respond to explosive attacks, including the coordination of Federal Government efforts with State, local, tribal, and territorial governments, first-responders, and private sector organizations. HSPD-19 required that the “Attorney General, in coordination with the Secretaries of Defense and Homeland Security and the heads of other Sector-Specific Agencies (as defined in HSPD-7) and agencies that conduct explosive attack detection, prevention, protection, or response activities ...develop an implementation plan.” HSPD-19 required that the plan implement its policy and any approved recommendations in the report and “include measures to (a) coordinate the efforts of Federal, State, local, territorial, and tribal government entities to develop related capabilities, (b) allocate Federal grant funds effectively, (c) resourced operational and tactical capabilities at each Federal department and agency with a role in homeland security; (d) coordinate training and exercise activities, and (e) incorporate, and strengthen as appropriate, existing plans and procedures to communicate accurate, coordinated, and timely information regarding a potential or actual explosive attack to the public, the media, and the private sector.”

The HSPD-19 report presents a holistic approach for improving the Nation’s ability to deter, prevent, detect, protect against, and respond to the threat of terrorist explosive and IED attacks on the homeland. The report provides 35 recommendations to enhance and align our current counter-IED capabilities and concludes that in order to improve our national CIKR protection posture, there must be a systematic approach in which all deterrence, prevention, detection, protection, and response efforts are unified. The strategy and recommendations provide a way forward that streamlines and enhances current activities, reducing conflict, confusion, and duplication of effort among interagency partners. The Implementation Plan builds on the policies, strategy, and guidance set forth by the President in HSPD-19 and outlined by the Attorney General and interagency partners in the HSPD-19 Report to the President.

The Secretary of Homeland Security designated IP to coordinate the department’s activities and represent DHS in the DOJ-led implementation of HSPD-19. IP efforts to enhance and coordinate the Nation’s ability to detect, deter, prevent, and respond to IED attacks against critical infrastructure, key resources, and soft targets include: (1) coordinating national and intergovernmental IED security efforts; (2) conducting requirements, capabilities, and gap analyses; and (3) promoting information-sharing and IED security awareness. DHS collaborated with DOJ to develop the Implementation Plan for Combating Terrorist Use of Explosives in the United States.

HSPD-19 also assigns to DHS specific roles and responsibilities for information sharing and counter-IED research, development, testing, and evaluation. HSPD-19 states that the Secretary of Homeland Security, in coordination with the Attorney General, the Director of National Intelligence, and the Secretaries of State and Defense, will establish and maintain secure information-sharing systems to provide law enforcement agencies and other first-responders with access to detailed information that enhances the preparedness of Federal, State, local, tribal, and territorial government personnel to deter, prevent, detect, protect against, and respond to explosive attacks in the United States.

Additionally, HSPD-19 states that the Secretary of Homeland Security, in coordination with the Attorney General, the Secretary of Defense, and the Director of the Office of Science and Technology Policy, is responsible for coordinating Federal Government research, development, testing, and evaluation activities related to the detection and prevention of, protection against, and response to explosive attacks and the development of explosives render-safe tools and technologies.

5.2 The CIKR Protection Component of the Homeland Security Mission

The result of this interrelated set of national authorities, strategies, and initiatives is a common, holistic approach to achieving the homeland security mission that includes an emphasis on preparedness across the board and on the protection of America's CIKR as a steady-state component of routine, day-to-day business operations for government and private sector partners.

The NIPP and NRF are complementary plans that span a spectrum of prevention, protection, response, and recovery activities to enable this coordinated approach on a day-to-day basis, as well as during periods of heightened threat. The NIPP and its associated SSPs establish the Nation's steady-state level of protection by helping to focus resources where investment yields the greatest return in terms of national risk management. The NRF addresses response and short-term recovery in the context of domestic threat and incident management. The National Preparedness Guidelines support implementation of both the NIPP and the NRF by establishing national priorities and guidance for building the requisite capabilities to support both plans at all levels of government.

Each of the guiding elements includes specific requirements for DHS and other Federal departments and agencies to build engaged partnerships and work in cooperation and collaboration with State, local, tribal, and private sector partners. This cooperation and collaboration between government and private sector owners and operators is specifically applicable to the CIKR protection efforts outlined in the NIPP.

The NIPP risk management framework, partnership model, and information-sharing mechanisms are structured to support coordination and cooperation between the public and private sectors while recognizing the differences between and within sectors, acknowledging the need to protect sensitive information, establishing processes for information sharing, and providing for smooth transitions from steady-state operations to incident response.

5.3 Relationship of the NIPP and SSPs to Other CIKR Plans and Programs

The NIPP and the SSPs outline the overarching elements of the CIKR protection effort that generally are applicable within and across all sectors. The SSPs are an integral component of the NIPP and exist as independent documents to address the unique perspective, risk landscape, and methodologies and approaches associated with each sector.

Homeland security plans and strategies at the State, local, and tribal levels of government address CIKR protection within their respective jurisdictions, as well as mechanisms for coordination with various regional efforts and other external entities. The NIPP also is designed to work with the range of CIKR protection-related plans and programs instituted by the private sector, both through voluntary actions and as a result of various regulatory requirements. These plans and programs include business continuity and resilience measures. NIPP processes are designed to enhance coordination, cooperation, and collaboration among CIKR partners within and across sectors to synchronize related efforts and avoid duplicative or unnecessarily costly security requirements.

5.3.1 Sector-Specific Plans

Based on guidance from DHS, the SSPs were developed jointly by the SSAs in close collaboration with the SCCs, GCCs, and others, including State, local, and tribal CIKR partners with key interests or expertise appropriate to the sector. The SSPs provide the means by which the NIPP is implemented across all sectors, as well as a national framework for each sector that guides the development, implementation, and updating of State and local homeland security strategies and CIKR protection programs. The SSPs for the original 17 sectors were officially released on May 21, 2007, after review and comment by the Homeland Security Council's Critical Infrastructure Protection Policy Coordination Committee. The SSP for the Critical Manufacturing Sector is under development and is scheduled for release in 2009.

Those SSPs that are available for general release may be downloaded from: <http://www.dhs.gov/nipp> (click on Sector-Specific Plans). If an SSP is not posted there, it is marked as FOUO. To request copies of the FOUO SSPs, please contact the responsible SSA, or the NIPP Program Management Office (NIPP@dhs.gov).

The SSPs are tailored to address the unique characteristics and risk landscapes of each sector while also providing consistency for protective programs, public and private protection investments, and resources. The SSPs serve to:

- Define sector partners, authorities, regulatory bases, roles and responsibilities, and interdependencies;
- Establish or institutionalize already existing procedures for sector interaction, information sharing, coordination, and partnership;
- Establish the goals and objectives, developed collaboratively among sector partners, that are required to achieve the desired protective posture for the sector;

- Identify international considerations;
- Identify areas for government action above and beyond an owner/operator or sector risk model; and
- Identify the sector-specific approach or methodology that SSAs use, in coordination with DHS and other sector partners, to conduct the following activities through the NIPP framework:
 - Identify priority CIKR and functions within the sector, including cyber considerations;
 - Assess sector risks, including potential consequences, vulnerabilities, and threats;
 - Assess and, as appropriate, prioritize assets, systems, networks, and functions of national-level significance within the sector;
 - Develop risk-mitigation programs based on detailed knowledge of sector operations and risk landscape;
 - Provide protocols to transition between steady-state CIKR protection and incident response in an all-hazards environment;
 - Use metrics to measure and communicate program effectiveness and risk management progress within the sector;
 - Address R&D requirements and activities relevant to the sector; and
 - Identify the process used to promote cooperation and information sharing within the sector.

The structure for the SSPs facilitates cross-sector comparisons and coordination by DHS and other SSAs.

5.3.2 State, Regional, Local, Tribal, and Territorial CIKR Protection Programs

The National Preparedness Guidelines define the development and implementation of a CIKR protection program as a key component of State, regional, local, tribal, and territorial homeland security programs. Creating and managing a CIKR protection program for a given jurisdiction entails building an organizational structure and mechanisms for coordination between government and private sector entities that can be used to implement the NIPP risk management framework. This includes taking action within the jurisdiction to: set goals and objectives; identify assets, systems, and networks; assess risks; set priorities for CIKR across sectors and jurisdictional levels; implement protective programs and resiliency

strategies; measure the effectiveness of risk management efforts; and share information among relevant public and private sector partners. These elements form the basis of focused CIKR protection programs and guide the implementation of the relevant CIKR protection-related goals and objectives outlined in State, local, and tribal homeland security strategies. To assist in the development of such CIKR protection programs, DHS issued a collaboratively developed Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal, and Territorial Levels (2008). The guide can be downloaded at www.dhs.gov/nipp.

In a regional context, the NIPP risk management framework and information-sharing processes can be applied through the development of a regional partnership model or the use of existing regional coordinating structures. Effective regional approaches to CIKR protection involve coordinated information sharing, planning, and sharing of costs. Regional approaches also include exercises to bring public and private sector partners together around: a shared understanding of the challenges to regional resilience; analytical tools to inform decisionmakers on risk and risk management, with the associated benefits and costs; and forums to enable decisionmakers to formulate protective measures and identify funding requirements and resources within and across sectors and jurisdictions.

State, regional, local, tribal, and territorial CIKR protection efforts enhance implementation of the NIPP and the SSPs by providing unique geographical focus and cross-sector coordination potential. To ensure that these efforts are consistent with other CIKR protection planning activities, the basic elements to be incorporated in these efforts are provided in appendix 5A. The recommended elements described in this appendix: recognize the variations in governance models across the States; recognize that not all sectors are represented in each State or geographical region; and are flexible enough to reflect varying authorities, resources, and issues within each State or region.

5.3.3 Other Plans or Programs Related to CIKR Protection

Federal partners should review and revise, as necessary, other plans that address elements of CIKR protection to ensure that they support the NIPP in a manner that avoids duplication and unnecessary layers of CIKR protection guidance. Examples of government plans or programs that may contain relevant prevention, protection, and response protocols or activities that relate to or affect CIKR protection include plans that address: State, local, and tribal hazard mitigation;

continuity-of-operations (COOP); continuity-of-government (COG); environmental, health, and safety operations; and integrated contingency operations. Review and revision of State, local, and tribal strategies and plans should be completed in accordance with overall homeland security and grant program guidance.

Private sector owners and operators develop and maintain plans for business risk management that include steady-state security and facility protection, as well as business continuity and emergency management plans. Many of these plans include heightened security requirements for CIKR protection that address the terrorist threat environment. Coordination with these planning efforts is relevant to effective implementation of the NIPP. Private sector partners are encouraged to consider the NIPP when revising these plans and to work with government partners to integrate their efforts with Federal, State, local, and tribal CIKR protection efforts, as appropriate.

5.4 CIKR Protection and Incident Management

Together, the NIPP and the NRF provide a comprehensive, integrated approach to addressing key elements of the Nation's homeland security mission to prevent terrorist attacks, reduce vulnerabilities, and respond to incidents in an all-hazards context. The NIPP establishes the overall risk-informed approach that defines the Nation's steady-state posture with respect to CIKR protection and resiliency, while the NRF and NIMS provide the overarching framework, mechanisms, and protocols required for effective and efficient domestic incident management. The NIPP risk management framework, information-sharing network, and partnership model provide vital functions that, in turn, inform and enable incident management decisions and activities.

5.4.1 The National Response Framework

The NRF provides an all-hazards approach that incorporates best practices from a wide variety of disciplines, including fire, rescue, law enforcement, public works, and emergency medical services. The operational and resource coordinating structures described in the NRF are designed to support decisionmaking during the response to a specific threat or incident and serve to unify and enhance the incident management capabilities and resources of individual agencies and organizations acting under their own authority. The NRF applies to a wide array of natural disasters, terrorist threats and incidents, and other emergencies.

The NRF core document and annexes, including the CIKR Support Annex, describe processes for coordination among:

various Federal departments and agencies; State, local, and tribal governments; and private sector partners, both for pre-incident preparedness, and post-incident response and short-term recovery. The NRF specifies incident management roles and responsibilities, including emergency support functions designed to expedite the flow of resources and program support to the incident area. The SSAs and other Federal departments and agencies have roles within the NRF structure that are distinct from, yet complementary to, their responsibilities under the NIPP. Ongoing implementation of the NIPP risk management framework, partnerships, and information-sharing networks sets the stage for CIKR security and restoration activities within the NRF by providing mechanisms to quickly assess the impact of the incident on both local and national CIKR, assist in establishing priorities for CIKR restoration, and augment incident-related information sharing.

5.4.2 Transitioning From NIPP Steady-State to Incident Management

The variety of alert and warning systems that exist for natural hazards, technological or industrial accidents, and terrorist incidents provide the bridge between steady-state operations using the NIPP risk management framework and incident management activities using the NRF concept of operations. These all-hazards alert and warning mechanisms include programs such as National Weather Service hurricane and tornado warnings, and alert and warning systems established around nuclear power plants and chemical stockpiles. In the context of terrorist incidents, HSAS provides a progressive and systematic approach that is used to match protective measures to the Nation's overall threat environment. This link between the current threat environment and the corresponding protective actions related to specific threat vectors or scenarios and to each HSAS threat level provides the indicators used to transition from the steady-state processes detailed in the NIPP to the incident management processes described in the NRF.

DHS and CIKR partners develop and implement stepped-up protective actions to match the increased terrorist threat conditions specified by HSAS, and to address various other all-hazards alerts and warning requirements. As warnings or threat levels increase, NRF coordinating structures are activated to enable incident management. DHS and CIKR partners carry out their NRF responsibilities and also use the NIPP risk management framework to provide the CIKR protection dimension of incident operations. The NRF CIKR Support Annex describes the concept of operations and details the activities needed to support public-private sector

incident operations and requirements, as well as to provide situational awareness, analysis, and prioritized recommendations to inform incident management decisions. When an incident occurs, regardless of the cause, the NRF is implemented for overall coordination of domestic incident management activities. The CIKR Support Annex includes a process for considering requests for assistance from CIKR owners and operators. Implementation of the CIKR Support Annex and the NIPP risk management framework facilitates those actions directly related to the current threat status, as well as incident prevention, response, and recovery. The NRF and CIKR Support Annex can be found at www.fema.gov/NRF.

The process for integrating CIKR protection with incident management and transitioning from NIPP steady-state processes to NRF incident management coordination includes the following actions by DHS, SSAs, and other CIKR partners:

- Increasing protection levels to correlate with the specific threat vectors or threat level communicated through HSAS or other relevant all-hazards alert and warning systems, or in accordance with sector-specific warnings using the NIPP information-sharing networks;
- Using the NIPP information-sharing networks and risk management framework to review and establish national priorities for CIKR protection; facilitating communications between CIKR partners; and informing the NRF processes regarding priorities for response and recovery of CIKR within the incident area, as well as on a national scale;
- Fulfilling roles and responsibilities as defined in the NRF for incident management activities; and
- Working with sector-level information-sharing entities and owners and operators on information-sharing issues during the active response mode.

In addition, the DHS Office of Public Affairs has an established communications protocol to facilitate timely information exchange and necessary coordination with the CIKR sectors and their Federal, State, local, and private sector partners during those national-level incidents that involve a coordinated Federal response.



6. Ensuring an Effective, Efficient Program Over the Long Term

This chapter addresses the efforts needed to ensure an effective, efficient CIKR protection program over the long term. It focuses particularly on the long-lead-time elements that require sustained plans and investments over time, such as generating skilled human capital, developing high-tech systems, and building public awareness.

Key activities needed to enhance CIKR protection and resiliency over the long term include:

- Building national awareness to support the CIKR protection program and related investments by ensuring a focused understanding of the all-hazards risk environment and what is being done to protect and enable the timely restoration of the Nation's CIKR in light of such threats;
- Enabling education, training, and exercise programs to ensure that skilled and knowledgeable professionals and experienced organizations are able to undertake NIPP-related responsibilities in the future;
- Conducting R&D and using technology to improve protective capabilities or resiliency strategies or to lower the costs of existing capabilities so that CIKR partners can afford to do more with limited budgets;
- Developing, protecting, and maintaining data systems and simulations to enable continuously refined risk assessment within and across sectors and to ensure preparedness for domestic incident management; and
- Continuously improving the NIPP and associated plans and programs through ongoing management and revision, as required.

6.1 Building National Awareness

DHS, in conjunction with the SSAs and other CIKR partners, is responsible for implementing a comprehensive national awareness program that focuses on public and private sector understanding of the CIKR all-hazards risk environment and motivates actions that support the sustainability of CIKR protection, investments, and risk management initiatives. Objectives of the CIKR national awareness program are to:

- Incorporate CIKR protection and restoration considerations into business planning and operations, including employee and senior manager education and training programs, across all levels of government and the private sector;
- Support public and private sector decisionmaking; enable relevant and effective strategic planning for CIKR protection and restoration; and inform resource allocation processes;
- Foster an understanding of:
 - CIKR dependencies and interdependencies, and the value of cross-sector CIKR protection and restoration planning down to the community level;
 - Evolving threats to CIKR as assessed by the intelligence community and in the context of HSAS; and

- Efforts to address the threat environment and enhance CIKR protection, resiliency, and rapid restoration.

DHS and other Federal agencies also engage in comprehensive national cyberspace security awareness campaigns to remove impediments to sharing vulnerability information among CIKR partners. This campaign includes audience-specific awareness materials, expansion of the Stay Safe Online campaign, and development of awards programs for those making significant contributions to the effort.

A Continuum of Capability Development

This document establishes a framework to enable awareness, education, training, and exercise programs that allow people and organizations to develop and maintain the core competencies and expertise required for effective implementation of the CIKR protection mission. Building the requisite individual and organizational capabilities requires attracting, training, and maintaining sufficient numbers of professionals who have the particular expertise unique or essential to CIKR protection. This, in turn, requires individual education and training to develop and maintain the requisite levels of competency through technical, academic, and professional development programs. It also requires organizational training and exercises to validate the processes and enhance the efficiency and effectiveness of CIKR programs.

As illustrated in figure 6-1, outreach and awareness create the foundation on which a comprehensive CIKR education and training program can be built. Exercises provide an objective assessment of an entity’s or individual’s capabilities, thus identifying areas for improvement and highlighting training gaps and needs.

The objectives of NIPP-related training and education programs are to:

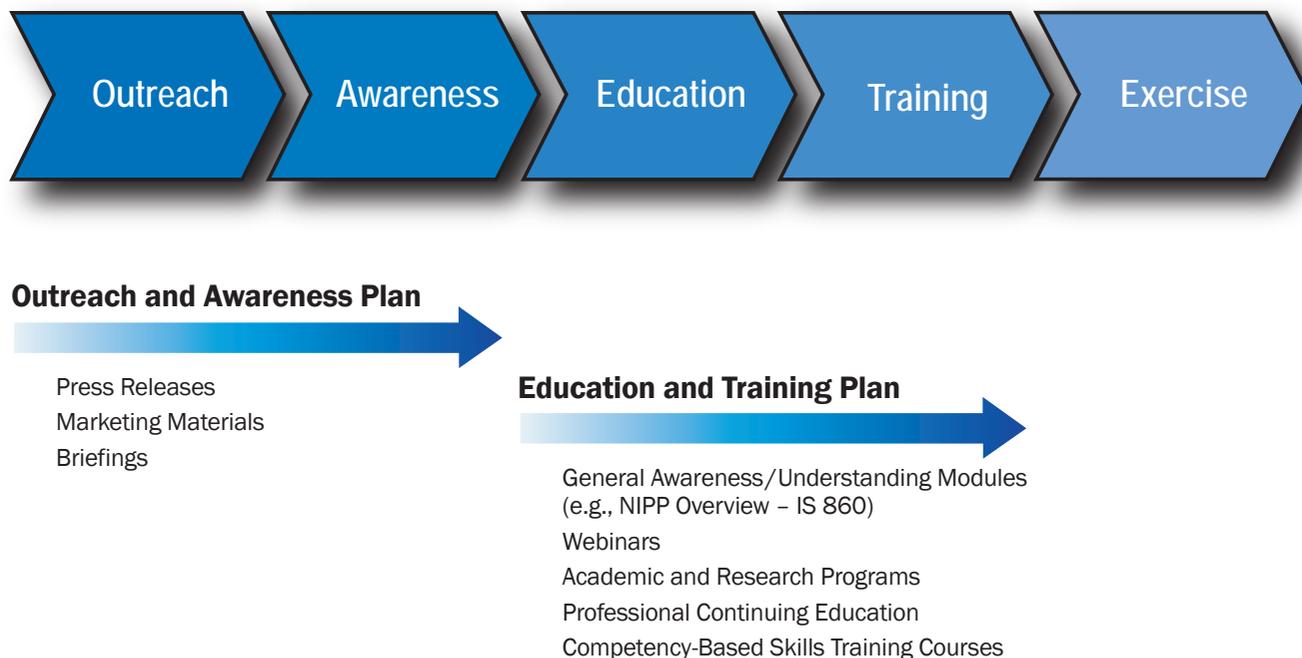
- Provide an integrated, coordinated approach to NIPP and CIKR-related education and training that energizes and involves all partners;
- Develop and implement grassroots education and training programs that communicate effectively with key audiences; and
- Maximize coordination, deepen relationships, and broaden the participation and practices required for implementing the NIPP and the SSPs.

The framework for education, training, and exercise is discussed below.

6.1.1 Education and Training

CIKR threat mitigation and protection have a broad target audience. Emphasis, for the purposes of education and training, is

Figure 6-1: Continuum of CIKR Capability Development



placed on these target audiences as collections of individuals rather than as organizations or entities, since it is the engagement and decisionmaking of those individuals, operating in their own areas of expertise and responsibility, that will determine the success of the public-private CIKR partnership.

It is crucial to understand these audiences and the similarities and differences among them in order to ensure the effective and efficient delivery of CIKR-related education and training. The following is a description of the primary CIKR training target audiences:

- State, local, tribal, and territorial government officials; SLTTGCC members; State elected officials; Homeland Security Directors and Advisors; emergency managers; program managers; and specialists;
- IP personnel, senior executives, program managers/analysts, PSAs, training managers, and specialists;
- The SSA and other Federal agency personnel; senior executives, program managers, and specialists;
- Regional consortium members;
- Owner/operator executives, security managers, program managers, and specialists; and

- Others, including international partner executives, security managers, program managers, and specialists.

6.1.2 Core Competencies for Implementing CIKR Protection

The U.S. Office of Personnel Management defines a competency as “a measurable pattern of knowledge, skills, abilities, behaviors, and other characteristics that an individual needs to perform work roles or occupational functions successfully.” A competency model is a collection of competencies that together define the elements required for performance. The CIKR competency model, illustrated in figure 6-2, provides the following:

- Define education and training requirements;
- Organize existing education and training efforts;
- Identify education and training gaps;
- Set forth a business case for education and training investments; and
- Establish performance metrics.

Each competency area is defined in table 6-1, which follows figure 6-2.

Figure 6-2: Developing CIKR Core Competencies

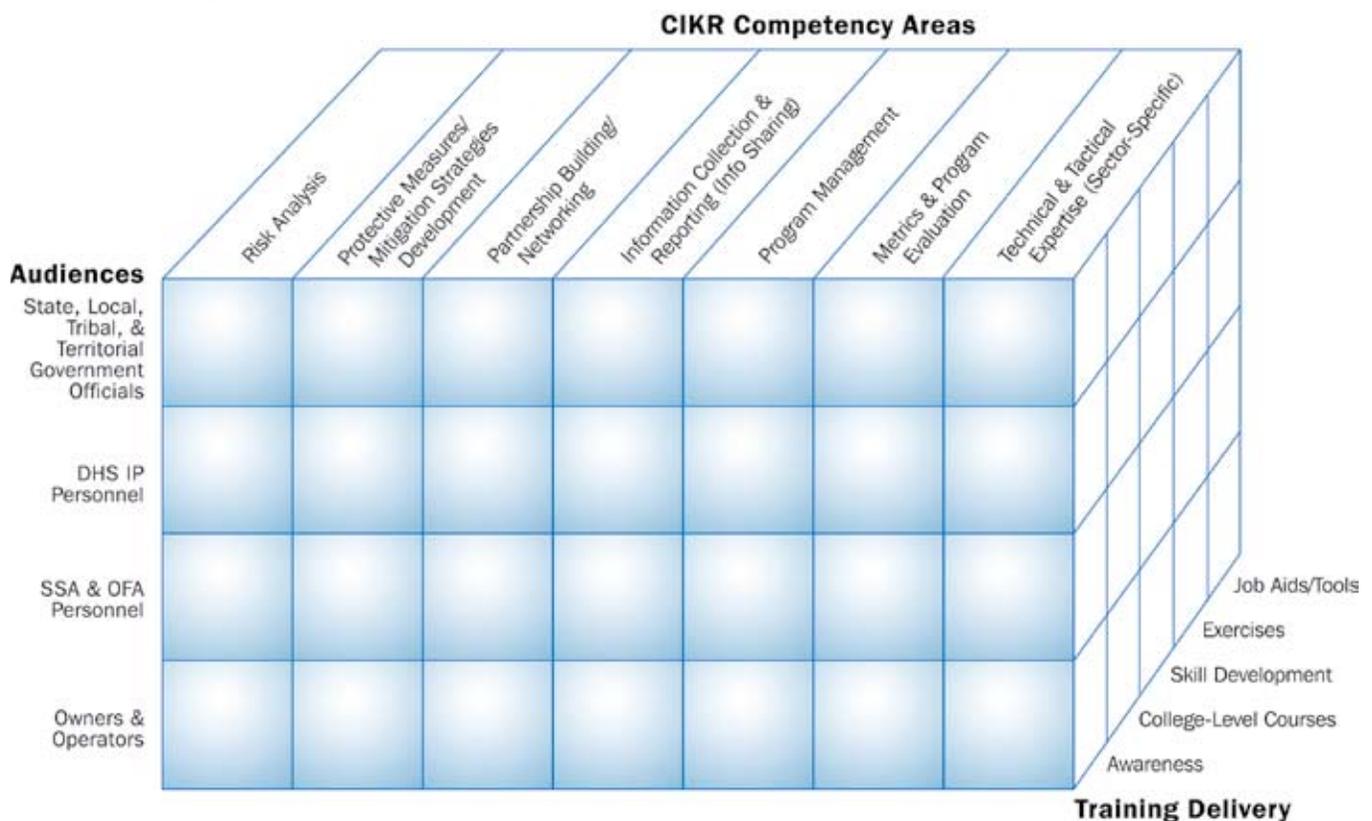


Table 6-1: CIKR Competency Areas

Area	Includes Knowledge and Skills To . . .
Risk Analysis	<ul style="list-style-type: none"> • Perform accurate, documented, objective, defensible, transparent, and complete analyses. • Support executive and managerial decisionmaking related to CIKR programs.
Protective Measures/ Mitigation Strategies	<ul style="list-style-type: none"> • Establish CIKR program goals and objectives based on risk analysis and risk-reduction return on investment. • Plan, develop, and implement CIKR-related projects, measures, and activities. Take advantage of existing emerging and anticipated methods and technologies in order to develop effective strategies, projects, and activities. • Implement continuous feedback mechanisms.
Partnership Building/ Networking	<ul style="list-style-type: none"> • Understand the roles and responsibilities of all partners. • Establish mechanisms for interacting with partners and exchanging information and resources (including best practices).
Information Collection & Reporting (Information Sharing)	<ul style="list-style-type: none"> • Use systems, tools, and protocols to collect, analyze, organize, report, and evaluate information. • Communicate and share information with sector partners at each tier of governance, including sector-specific, across sectors, and within the private sector.
Program Management	<ul style="list-style-type: none"> • Establish sector-specific or jurisdictional CIKR goals and plans. • Identify and prioritize CIKR projects, strategies, and activities for a sector or jurisdiction. • Manage a CIKR program on schedule, within budget, and in compliance with performance standards. • Design and implement continuous feedback mechanisms at the program level. • Develop and implement CIKR training plans.
Metrics & Program Evaluation	<ul style="list-style-type: none"> • Define and establish CIKR metrics based on goals and objectives. • Establish data collection and measurement plans, systems, and tools. • Collect and analyze data. • Report findings and conclusions.
Technical & Tactical Expertise (Sector- Specific)	<ul style="list-style-type: none"> • Note: This area includes the specialized (sector-specific) expertise required to plan, implement, and evaluate technical and tactical activities, measures, and programs.

The training delivery levels identified in figure 6-2 represent a cumulative structure that begins with basic awareness and progresses to the expert knowledge and skills required to perform specific CIKR-related tasks and functions. Training and education programs typically fall into these levels:

- **Awareness Materials:** Motivate or inform course participants about CIKR-related concepts, principles, policies, or procedures.
- **College Courses:** Present advanced CIKR knowledge, research, and theories to promote professional development.
- **Skill Development Sessions:** Focus on improving the performance of specific CIKR functions and tasks, both during training and in the workplace.
- **Exercises:** Reinforce and test CIKR skill acquisition, processes, and procedures.
- **Job Aids:** Include tools or resources (such as guides, checklists, templates, and decision aids) that allow an individual to quickly access the CIKR information that he/she needs to perform a task.

6.1.3 Individual Education and Training

Building and sustaining capabilities to implement the NIPP involves a complex approach to the education and training effort that leverages existing accredited academic programs, professional certification standards, and technical training programs. This requires an effort with a national scope that includes, but is not limited to, the following components:

- Training to provide individuals with the skills needed to perform their roles and responsibilities under the NIPP and the SSPs;
- Academic and research programs that result in formal degrees from accredited institutions; and
- Professional continuing education, which incorporates the latest advances in CIKR risk-mitigation approaches and, where appropriate, certification based on government, industry, and professional organization standards.

To enable each of these components, the specific areas of emphasis are discussed in the subsections that follow.

6.1.3.1 CIKR Protection Training

DHS, SSAs, and other CIKR partners offer a wide array of training programs designed to enhance core competencies and build the capabilities needed to support NIPP and SSP implementation among the various target audiences. The level and content of training programs vary based on sector require-

ments. Some sectors rely on the use of established training programs, while others develop courses to meet specific tactical or technical objectives. DHS offers NIPP-awareness-level training through the FEMA Emergency Management Institute (EMI). The independent study course (IS 860) is available online or for classroom delivery. This course provides a foundation of the basic principles of the NIPP, including the risk management framework and partnership model, information sharing, and roles and responsibilities.

DHS, SSAs, and other CIKR partners offer courses that enhance CIKR protection. One of the ongoing objectives of NIPP- and SSP-related training is to identify and align training that enhances the core competencies and provides the appropriate level of training and development opportunities for each of the identified training audiences.

NIPP and SSP-related training and education programs, to date, focus on enhancing risk management, information collection, and the tactical and technical competencies required to detect, deter, defend, and mitigate against terrorist activities and other incidents. DHS and other Federal agencies support and provide training resources to local law enforcement and others, with a special focus on urban areas with significant clusters of CIKR, localities where high-profile special events are typically scheduled, or other potentially high-risk geographical areas or jurisdictions. Federally provided technical training covers a range of topics such as buffer zone protection, bombing prevention, workforce terrorism awareness, surveillance detection, high-risk target awareness, WMD incident training, and continuity-of-operations training.

DHS supports cybersecurity training, education, and awareness programs by educating vendors and manufacturers on the value of: pre-configuring security options in products so that they are secure on initial installation; educating users on secure installation and use of cyber products; increasing user awareness and ease of use of the security features in products; and, where feasible, promotion of industry guidelines. These training efforts also encourage programs that leverage the existing Federal Cyber Service: Scholarship for Service Program, as well as various graduate and post-doctoral programs; link Federal cybersecurity and computer forensics training programs; and establish cybersecurity programs for departments and agencies, including awareness, audits, and standards, as required.

DHS solicits recommendations from national professional organizations and from Federal, State, local, tribal, and private sector partners for additional discipline-specific technical training courses related to CIKR protection and supports course development, as appropriate.

6.1.3.2 Academic Programs

DHS works with a wide range of academic institutions to incorporate CIKR protection into professional education programs with majors or concentrations in this mission area. DHS collaborates with universities to incorporate homeland security-related curriculum, sponsors a post-graduate level program at the Naval Postgraduate School in homeland defense and security, and collaborates with other higher education programs. These venues offer opportunities to incorporate concentrations in various aspects of CIKR protection as part of the multidisciplinary degree programs.

DHS is promoting the development of a long-term higher education program that will include academic degrees and adult education. The program is being developed through a collaborative effort involving the IP, the S&T Universities and Centers for Excellence Programs, TSA, and others. The initial program is being developed in conjunction with the National Transportation Security Center for Excellence (NTSCOE), which brings together a number of academic institutions with a mandate to build education and training programs relevant to the CIKR protection mission. This initiative provides the framework for the identification, development, and delivery of critical infrastructure courses for the transportation industry. The initiative will lead to the implementation of adult education and academic degree programs as part of a multidisciplinary core curriculum applicable across all critical infrastructure sectors.

DHS will examine existing cybersecurity programs within the research and academic communities to determine their applicability as models for CIKR protection education and broad-based research. These programs include:

- Co-sponsorship of the National Centers of Academic Excellence in Information Assurance Education (CAEIAE) and CAE research programs with the National Security Agency; and
- Collaboration with the National Science Foundation to co-sponsor the Federal Cyber Service: Scholarship for Service Program. The Scholarship for Service Program provides grant money to selected CAEIAE universities to fund the final 2 years of student bachelor's, master's, or doctoral study in information assurance in exchange for an equal amount of time spent working for the Federal Government.

DHS will ensure that the NCIP R&D Plan appropriately considers the human capital needs for protection-related R&D by incorporating analysis of the research community's future need for advanced degrees in protection-related disciplines into the plan development process.

6.1.3.3 Continuing Education and Professional Competency

DHS encourages the use of established professional standards where practical and, when appropriate, works with CIKR partners to facilitate the development of continuing education, professional competency programs, and professional standards for areas requiring unique and critical CIKR protection expertise. For example, DHS is fostering the development of CIKR adult and continuing education programs and leading the development of private sector preparedness standards that are relevant to the CIKR protection mission.

The adult education initiative focuses on enhancing the skills and abilities of CIKR professionals and employees at all levels in order to provide:

- General awareness and baseline understanding of critical infrastructure, preparedness, and protective measures; and
- Specialized CIKR training for individuals directly engaged in jobs or activities related to CIKR protection (security, business continuity, emergency management, IT, engineering, and others).

6.1.4 Organizational Training and Exercises

Building and maintaining organizational and sector expertise requires comprehensive exercises to test the interaction between the NIPP and the NRF in the context of terrorist incidents, natural disasters, and other emergencies. Exercises are conducted by private sector owners and operators, and across all levels of government. They may be organized by these entities on a sector-specific basis or through the NEP. Through the NEP Training and Exercise Planning Workshop, CIKR exercises can be nominated for inclusion on the NEP Five-Year Exercise Schedule. IP, in collaboration with the SSAs and the CIKR Cross-Sector Council, serves as the conduit for all 18 CIKR sectors' participation in NEP-sponsored activities and events. As such, the IP exercise program strictly adheres to the tenets of the NEP. CIKR-related exercise planning and NIPP partner participation is coordinated within IP through its Exercise Working Group (EWG), which consists of representation from all IP projects, the SSAs, and the private sector. The EWG allows NIPP partners to translate goals and priorities into specific objectives, coordinate exercise activities, participate in the planning and conduct of exercises, and track improvement plan actions against current capabilities, training, and exercises. This group is also responsible for maintaining the IP Multi-Year Training and Exercise Plan. This document is assessed and revised, as needed, on an annual basis at the IP Training and Exercise Planning Workshop.

National Exercise Program

DHS provides overarching coordination for the NEP to ensure the Nation's readiness to respond in an all-hazards environment and to test the steady-state protection plans and programs put in place by the NIPP and their transition to the incident management framework established in the NRF.

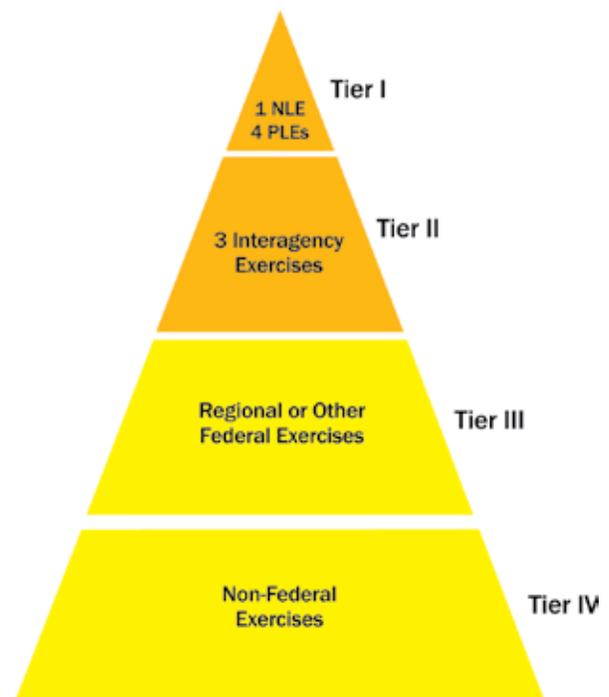
Terms used by the NEP program include:

- **National Level Exercise (NLE)**—an annual national security and/or homeland security exercise centered on White House-directed, U.S. Government-wide strategy and policy.
- **Principal Level Exercise (PLE)**—a quarterly exercise, for appropriate department and agency principals or their deputies, focused on current U.S. Government-wide strategic issues.
- **NEP Five-Year Exercise Schedule**—identifies the strategic focus and scenario of each NEP Tier 1 and II exercise that includes a strategic U.S. Government-wide focus.
- **National Exercise Schedule (NEXS)**—a schedule of all Federal, State, and local exercises.
- **Corrective Action Program (CAP)**—administered by DHS in support of the Homeland Security Council (HSC) and the National Security Council (NSC), involves a system and process for identifying, assigning, and tracking the remediation of issues.
- **Homeland Security Exercise and Evaluation Program (HSEEP)**—DHS policy and guidance for designing, developing, conducting, and evaluating exercises. Provides a threat and performance-based exercise process that includes a mix and range of exercise activities through a series of four reference manuals to help States and local jurisdictions establish exercise programs and design, develop, conduct, and evaluate exercises.

The NEP categorizes exercise activities into four tiers, as shown in figure 6-3. These tiers reflect the relative priority for national and regional Federal interagency participation, with NEP Tier I as the highest and NEP Tier IV as the lowest. U.S. Government exercises are assigned to NEP tiers based on a consensus interagency judgment of how closely they align to U.S. Government-wide strategic and policy priorities.

- **Tier I Exercises (Required):** NEP Tier I exercises are centered on White House directed, U.S. Government-wide strategy and policy-related issues and are executed with the participation of all appropriate department and agency principals (or their deputies) and all necessary operations

Figure 6-3: National Exercise Program Tiers



centers, nationally and regionally as appropriate. NLEs and Principal-Level Exercises (PLEs) constitute NEP Tier I and there are five NEP Tier I exercises annually.

- **Tier II Exercises (Commended):** NEP Tier II exercises are focused on strategy and policy issues supported by all appropriate departments and agencies, either through the National Exercise Simulation Cell or as determined by each department or agency's leadership. NEP Tier II exercises are endorsed through the NEP process as meriting priority for interagency participation. NEP Tier II exercises take precedence over NEP Tier III exercises in the event of resource conflicts. The Exercise and Evaluation Sub-Policy Coordination Committee shall recommend no more than three NEP Tier II exercises for interagency participation annually.
- **Tier III Exercises (Permitted):** NEP Tier III exercises are other Federal exercises focused on plans, policies, procedures, and objectives at the operational, tactical, or organization-specific level that do not require broad interagency headquarters-level involvement to achieve their stated exercise or training objectives.
- **Tier IV Exercises:** NEP Tier IV exercises are exercises in which State, local, tribal, and/or territorial governments, and/or private sector entities are the primary training audience or the subject of evaluation.

DHS chairs and facilitates the NEP Executive Steering Committee (ESC). The NEP ESC coordinates department and agency, as well as regional, State, and local exercise requirements and objectives, and builds a recommended NEP Five-Year Exercise Schedule. The NEP ESC also prioritizes recommended lessons learned and corrective action plans. The core members include DHS, DoD, DOE, HHS, DOJ, DOS, DOT, the Office of the Director of National Intelligence (ODNI), and the FBI. There are up to three rotating members serving 1-year terms. HSC, NSC, and OMB representatives serve in a non-voting oversight capacity. The recommended NEP Five-Year Exercise Schedule and CAP are submitted to the Deputies for approval through the Domestic Response Group Exercise and Evaluation Policy Coordination Subcommittee to frame those decisions.

Capabilities-Based Planning

The NEP has adopted a capabilities-based approach to exercise program management, foundation, design, development, conduct, evaluation, and improvement planning. Capabilities-based planning builds capabilities suitable for a wide range of threats and hazards while working within an economic framework that necessitates prioritization and choice. It addresses uncertainty by analyzing a wide range of realistic scenarios to identify required capabilities, and is the basis for guidance such as the National Preparedness Guidelines, Target Capabilities List (TCL), and Universal Task List (UTL). Capabilities-based planning is incorporated throughout the cycle of preparedness, to include plans, training, equipment, as well as exercises.

Training and Exercise Outreach and Coordination

DHS, SSAs, SCC, GCC, owners and operators, and other CIKR partners work together to ensure that exercises include adequate testing of steady-state CIKR protection measures and plans, including: information sharing; application of the NIPP risk management framework; and the ability of a protected core of life-critical CIKR services, such as power, food and water, and emergency transportation, to withstand attacks or natural disasters and continue to function at an appropriate level. DHS also ensures that the NIMS Integration Center, which serves as the repository and clearinghouse for reports and lessons learned from actual incidents, training, and exercises, regularly compiles and disseminates information on CIKR protection best practices.

In an effort to better familiarize its State, regional, local, tribal, territorial, and private sector partners with the NIPP, IP hosts an annual series of NEP Tier III, NIPP-related workshops and tabletop exercises. The goals for this series include

increasing the understanding of: the NIPP; the IP organization, as well as non-IP SSAs; IP critical points of entry for public and private partners; State, regional, local, tribal, and territorial organizations' CIKR protection programs; and private sector CIKR protection activities, as well as identifying gaps and redundancies in these CIKR protection efforts.

6.1.5 CIKR Partner Role and Approach

Given the scope and nature of the education, training, and exercise needs related to CIKR protection, the approach adopted must, to the greatest extent possible, leverage existing education, training, and exercise programs.

DHS works through the NIPP partnership structure to provide awareness-level training to introduce public and private sector partners to the NIPP contents and requirements, and other core curriculum that provides a cross-sector basis for CIKR program management, sector awareness, metrics, and other content relevant for all sectors and jurisdictions. DHS encourages and, where appropriate, facilitates specialized NIPP-related occupational and professional training and education, and development of professional and personnel security guidelines. It also will encourage academic and research programs, and coordinate the design of exercises that test and validate the interaction between the NIPP framework and the NRF.

The SSAs and other Federal agencies are responsible for reviewing, updating, and, as appropriate, developing new CIKR protection-related training and education programs that align with the NIPP and the competency model. Other CIKR partners are encouraged to review existing training and/or develop new training to align with the competency model and support implementation of the NIPP, the SSPs, and/or identified CIKR protection needs within their jurisdiction. All CIKR partners should work with DHS and the SSAs to identify and fill gaps in current training, education, and exercise programs for those specialized disciplines that are unique to CIKR protection and resiliency.

6.2 Conducting Research and Development and Using Technology

HSPD-7 establishes the national policy for “enhancing protection of the Nation’s critical infrastructure and key resources” and mandates plans to: systematically “harness the Nation’s research and development capabilities”; provide the long-term technology advances needed for more effective and cost-efficient protection of CIKR; and provide the sustained science, engineering, and technology base needed to prevent

or minimize the impact of future attacks on our physical and cyber infrastructure systems.

Protection of the Nation's physical and cyber infrastructure and the people who operate and use these vital systems is an extremely challenging portion of the overall homeland security effort. The national architecture of CIKR assets and systems continually grow more complex and more interdependent. Therefore, plans must cut across a broad range of sectors, Federal and non-Federal governmental entities, and critical industries.

Federal agencies work collaboratively to design and execute R&D programs to help develop knowledge and technology that can be used to more effectively mitigate the risk to CIKR. Congress has provided for liability protections under the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act) that serve to encourage technology use by CIKR partners.

In the near term, risk-informed priorities are designed to allocate resources where they can best mitigate risk or improve resiliency. In the long term, R&D holds the key to more effective and cost-efficient CIKR protection and resiliency through advances in technology. R&D programs work to improve all aspects of CIKR protection—from the detection of threats, through protection and performance measures, to inherently secure and more resilient advanced infrastructure designs.

Because owners and operators play a major role in CIKR protection, research programs that support the NIPP must find effective ways to consider the perspectives of sector professional associations, sector councils, and other sources that understand owner and operator technology needs.

Unique R&D needs associated with CIKR protection include:

- Conducting the development or redesign of technology-based equipment to significantly lower the costs of existing capabilities so that CIKR partners with limited budgets can afford state-of-the-art solutions;
- Researching issues, such as resiliency and protection in building design, that affect all CIKR and can result in solutions that can provide benefits across sectors if implemented; and
- Focusing research on the implementation and operational aspects of technology used for CIKR protection to provide resources that can help inform technology investment decisions, such as technical evaluation of security equipment or technology clearinghouse information.

6.2.1 The SAFETY Act

Ingenuity and invention are the lifeblood of robust R&D. But potential liabilities could stifle the entrepreneurial spirit for developing technologies and products that disrupt attacks and enable effective response. As part of the Homeland Security Act, Public Law 107-296, Congress enacted the SAFETY Act, which creates liability protections for sellers of qualified anti-terrorism technologies. The SAFETY Act provides incentives for the development and deployment of anti-terrorism technologies by limiting liability through a system of risk and litigation management. The purpose of the SAFETY Act is to ensure that the threat of liability does not deter potential sellers of anti-terrorism technologies from developing, deploying, and commercializing technologies that could save lives. The SAFETY Act gives liability protection to both sellers of qualified anti-terrorism technology and their customers, and applies to all types of enterprises that develop, sell, or use anti-terrorism technologies.

The SAFETY Act applies to a broad range of technologies, including products, services, and software, or combinations thereof, as well as technology firms and providers of security services. The SAFETY Act protects those businesses and their customers and contractors by providing a series of liability protections if their products or services are found to be effective by the Secretary of Homeland Security. Additionally, if the Secretary certifies the technology under the SAFETY Act (i.e., that the technology actually performs as it is intended to do and conforms to certain seller specifications), the seller is afforded a complete defense in litigation related to the performance of the technology in preventing, detecting, or deterring terrorist acts or deployment to recover from one. Those technologies that have been "certified" are placed on an Approved Product List for Homeland Security that is available at www.safetyact.gov.

A clear benefit of the SAFETY Act is that a cause of action may be brought only against the seller of the Qualified Anti-Terrorism Technology and may not be brought against the buyer(s), their contractors, or downstream users of the Qualified Anti-Terrorism Technology, or against the seller's suppliers or contractors. This stipulation includes CIKR owners and operators.

CIKR facility owners and operators are encouraged to examine the SAFETY Act closely because: (1) CIKR owners (if purchasers of qualified technologies) will enjoy the liability protections that flow from using qualified SAFETY Act technologies, and (2) CIKR owners will also have a level of assurance that the qualified products and services that

they are utilizing have been vetted by DHS. Lower liability insurance burdens for those using qualified technologies are another potential outcome.

In these ways, the SAFETY Act is a valuable tool that can enhance the ability of owners and operators to protect our Nation's CIKR.

6.2.2 National Critical Infrastructure Protection R&D Plan

As directed by HSPD-7, the Secretary of Homeland Security works with the Director of OSTP, EOP, to develop the NCIP R&D Plan as a vehicle to support implementation of CIKR risk management and supporting activities and programs.

The NCIP R&D Plan provides the focus and coordination mechanisms required to achieve the vision provided in the President's Physical and Cyber Security CIKR Protection Strategies. That vision calls for a "systematic national effort to fully harness the Nation's research and development capabilities." The R&D planning process is designed to address common issues faced by the various sector partners and to ensure a coordinated R&D program that yields the greatest value across a broad range of interests and requirements. The plan addresses both physical and cyber CIKR protection. The planning process also provides for the revision of research goals and priorities over the long term to respond to changes in the threat, technology, environment, business continuity, and other factors.

DHS and OSTP coordinate with Federal and private sector partners, including academic and national laboratory representatives, during the R&D planning cycle. The interagency process used to develop and coordinate this plan is managed through the Infrastructure Subcommittee of the National Science and Technology Council (NSTC), which is co-chaired by DHS and OSTP. The SSAs are responsible for providing input into the plan after coordination with sector representatives and experts through such bodies as the SCCs and GCCs.

The NCIP R&D Plan articulates strategic R&D goals and identifies the R&D areas in which advances in CIKR protection must be made. The goals and cross-sector R&D areas contained in the NCIP R&D Plan are discussed in the following subsections.

6.2.2.1 CIKR Protection R&D Strategic Goals

The NCIP R&D planning process identifies three long-term, strategic R&D goals for CIKR protection:

- A common operating picture to continuously monitor the health of CIKR;

- A next-generation Internet architecture with designed-in security; and
- Resilient, self-diagnosing, self-healing infrastructure systems.

The strategic goals are used to guide Federal R&D investment decisions and also to provide a coordinated approach to the overall Federal research program. S&T and OSTP will work with OMB to use the R&D Plan as a decisionmaking tool for the evaluation of budget submissions across Federal agencies. These goals also help guide the programs of researchers who receive Federal grants and contracts.

6.2.2.2 CIKR Protection R&D Areas

R&D development projects for CIKR protection programs fall into nine R&D areas or themes that cut across all CIKR sectors:

- Detection and sensor systems;
- Protection and prevention systems;
- Entry and access portals;
- Insider threats;
- Analysis and decision support systems;
- Response and recovery tools;
- New and emerging threats and vulnerabilities;
- Advanced infrastructure architectures and systems design; and
- Human and social issues.

Organizing research in these areas enables the development of effective solutions that may be applied across sectors and disciplines. These themes also provide an organizing framework for SSA use during the development of R&D requirements for their respective sectors, which will be reflected in the SSPs. These requirements specify the capabilities that each sector needs to satisfy CIKR protection needs. By incorporating these requirements into the NCIP R&D Plan, OMB is better able to ensure that agency R&D budget requests are aligned with the National R&D Plan for CIKR Protection. Requirements are refreshed each year through the sector annual reporting process.

6.2.2.3 Coordination of the NCIP R&D Plan With SSP and Sector Annual Report R&D Planning

Each SSP includes a section on sector-specific CIKR protection R&D that explains how the sector will strengthen the linkage among sector-specific and national R&D planning efforts, technology requirements, current R&D initiatives, gaps, and candidate R&D initiatives. New candidate R&D initiatives are developed during the Sector Annual Report writing process. The SSP explains the process for:

- **Sector Technology Requirements:** Identifying and providing a summary of sector technology requirements and communicating them to IP, S&T, and OSTP for inclusion in the NCIP R&D Plan on an annual basis;
- **Current R&D Initiatives:** Annually soliciting a listing of current Federal R&D initiatives from the S&T and OSTP that have the potential to meet sector CIKR protection challenges and providing a description of how this listing will be analyzed to indicate which initiatives have the greatest potential for a positive impact;
- **Gaps:** Conducting an analysis of the gaps between the sector's technology needs and current R&D initiatives from the S&T and OSTP; and
- **Candidate R&D Initiatives:** Determining which candidate R&D initiatives are most relevant for the sector and how these will be summarized and reported to all appropriate stakeholders.

Each SSA coordinates the development of the sector R&D planning component of their SSP and SAR so that these documents reflect the SSA's sector-level R&D investment priorities. Coordination between IP, S&T, and the sectors through the SSAs, GCCs, and SCCs ensures that the R&D information in the SSP and Sector Annual Report is comprehensive.

6.2.3 Other R&D That Supports CIKR Protection

Other R&D efforts that may support CIKR protection are conducted by the SSAs and other Federal agencies. These programs address the research requirements set forth in the President's Physical and Cyber Security CIKR Protection Strategies, which call for:

- Ensuring the compatibility of communications systems with interoperability standards;
- Exploring methods to authenticate and verify personal identity;
- Coordinating the development of CIKR protection consensus standards; and
- Improving technological surveillance, monitoring, and detection capabilities.

For example, the Technical Support Working Group is the U.S. national forum that identifies, prioritizes, and coordinates interagency and international R&D requirements for combating terrorism. The Technical Support Working Group rapidly develops technologies and equipment to meet the high-priority needs of the anti-terrorism community,

including efforts that can contribute to CIKR protection, and addresses joint international operational requirements through cooperative R&D with major allies.

DHS also conducts cooperative R&D programs with other Federal agencies related to authentication and verification of personal identity for the CIKR protection workforce and works with the American National Standards Institute and the National Institute of Standards and Technology (NIST) through the Homeland Security Standards Panel to help coordinate the development of consensus standards that support CIKR protection.

6.2.4 DHS Science and Technology Strategic Framework

The Homeland Security Act of 2002 gave S&T the responsibility of advising the DHS Secretary on S&T requirements, priorities, and programs that support the department's vision and mission. The directorate also has the responsibility of developing and integrating technology with the strategies, policies, and procedures in order to protect the Nation's CIKR.

CIKR requirements are mapped to Integrated Product Teams (IPTs) managed by S&T. S&T focuses on enabling its customers—the DHS components—and their customers, including: Border Patrol agents; the Coast Guard; airport baggage screeners; Federal Air Marshals; and State, local, and Federal emergency responders, as well as the many others teamed and committed to the vital mission of securing the Nation. Other CIKR customers of S&T are the sectors and their partners who own and operate infrastructure. Sectors develop long-term requirements that are documented in SSPs. Sector Annual Reports update requirements in response to changes in risk as advised by the annual National Risk Profile. The National Annual Report further applies the National Risk Profile to prioritize requirements across sectors.

To reach its goals, S&T created a customer-focused, output-oriented, full-service S&T management organization. See appendix 6 for a detailed discussion of the S&T organization as it relates to CIKR technology development.

6.2.5 Transitioning Requirements Into Reality

After identifying and justifying risk-based R&D requirements in the Sector CIKR Protection Annual Reports, the full set of requirements are reviewed, summarized, and consolidated to develop the set presented in the National CIKR Protection Annual Report. DHS works with the SSAs, SCCs, GCCs, and cross-sector councils to further validate and refine the requirements and to prioritize them before submitting them

to the IPT process. The different IPTs then work to define the actual projects, identify costs and resources, and finally turn them into S&T projects.

Specifically, IPTs coordinate the planning and execution of R&D programs together with the eventual hand-off to the maintainers and users of the project results. The IPTs are critical nodes in the process to determine operational requirements, assess current capabilities to meet operational needs, analyze gaps in capabilities and articulate programs and projects to fill in the gaps and expand competencies.

IPTs constitute the Transition portfolio of S&T, targeting deployable capabilities in the near term. IPTs generally include the research and technology perspective, the customer/end-user perspective, and an acquisitions perspective. The customers/end-users monitor and guide the capability being developed; the research and technology representatives inform the discussions with scientific and engineering advances and emerging technologies; and the acquisitions staff helps to transition the results into practice by the maintainers and the end-users of the capability.

The overall requirements process promotes rigor in the analysis and prioritization of sector requirements and capability gaps and also provides feedback to sectors on how their needs align with ongoing and planned S&T projects.

6.3 Building, Protecting, and Maintaining Databases, Simulations, and Other Tools

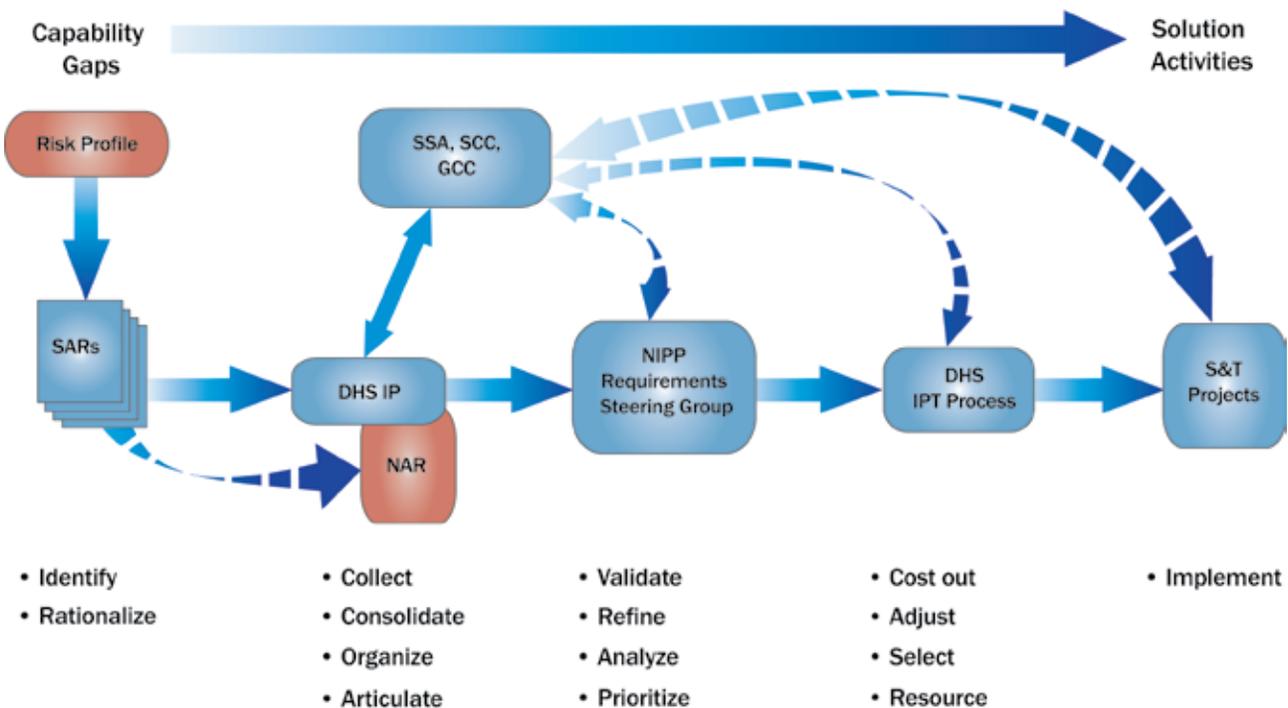
Many data systems, databases, models, simulations, decision support systems, and similar information tools currently exist or are under development to enable the execution of national CIKR risk management.

To keep pace with the constantly evolving threat, technology, and business environments, these tools must be updated and, in some cases, new tools must be developed. Sensitive information associated with these tools must be appropriately protected. Priority efforts in this area will be focused on updating and improving key databases, developing and maintaining simulation and modeling capabilities, and coordinating with CIKR partners on databases and modeling.

6.3.1 National CIKR Protection Data Systems

HSPD-7 directs the Secretary of Homeland Security to implement plans and programs that identify, catalog, prioritize, and protect CIKR in cooperation with all levels of government and private sector entities. Data systems currently provide the capability to catalog, prioritize, and protect CIKR through such functions as:

Figure 6-4: The NIPP R&D Requirements Generation Process



- Maintaining an inventory of asset information and estimating the potential consequences of an attack or incident (e.g., the IDW);
 - Storing information related to terrorist attacks or incidents (e.g., the National Threat and Incident Database);
 - Analyzing dependencies and interdependencies (e.g., the NISAC);
 - Managing the implementation of various protective programs (e.g., the BZPP Request Database); and
 - Providing the continuous maintenance and updates required to enable data in these systems to reflect changes in actual circumstances, using tools such as iCAV and DHS Earth.
- Work with end-users to design operations-related tools that provide maximum utility and clarity for CIKR protection activities in both emergencies and routine operations;
 - Work with end-users to design appropriate information protection plans for sensitive information used and produced by CIKR protection modeling tools;
 - Provide guidance on the vetting of modeling tools to include the use of private sector operational, technical, and business expertise, where appropriate; and
 - Review existing private sector modeling initiatives and opportunities for joint ventures to ensure that DHS, the SSAs, and their CIKR partners make the maximum use of applicable private sector modeling capabilities.

Properly maintaining systems with current and useful data involves long-term support, coordination, and resource commitments by DHS, the SSAs, the States, private sector entities, and other partners.

6.3.2 Simulation and Modeling

A number of CIKR partners make use of models and simulations to comprehensively examine the potential consequences from terrorist attacks, natural disasters, and manmade accidents that affect CIKR, including the effects of sector and cross-sector dependencies and interdependencies. Continuous maintenance and updates are required for these tools to produce reliable projections. Over the long term, new tools are needed to address fundamental changes due to factors such as technology, threats, or the business environment.

IP is the lead coordinator for modeling and simulation capabilities regarding CIKR protection and resiliency. In this capacity, DHS will:

- Coordinate with the S&T on requirements for the development, maintenance, and application of research-related modeling capabilities for CIKR protection and resiliency;
- Specify requirements for the development, maintenance, and application of operations-related modeling capabilities for CIKR protection in coordination with S&T and the SSAs, as appropriate;
- Coordinate with the SSAs that have relevant modeling capabilities to develop appropriate mechanisms for the development, maintenance, and use of such for CIKR protection as directed by HSPD-7;
- Familiarize the SSAs and other CIKR partners with the availability of relevant modeling and simulation capabilities through training and exercises;

The principal modeling, simulation, and analysis capability within the IP is the NISAC. NISAC analysts and operational resources are located at the Sandia and Los Alamos National Laboratories and the program operates under the direction of a Washington, DC-based program office within IP. Mandated by Congress to be a “source of National Expertise to address critical infrastructure protection” research and analysis, NISAC prepares and shares analyses of CIKR, including their interdependencies, vulnerabilities, the consequences of loss, and other complexities. NISAC has developed tailored analytical tools, a core of unique expertise, and procedures designed to effectively address the strategic-level analytical needs of CIKR decisionmakers.

While the 2001 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act established the requirement for NISAC, the Homeland Security Appropriations Act of 2007 specifies its current mission. NISAC is required to provide “modeling, simulation, and analysis of the assets and systems comprising CIKR in order to enhance preparedness, protection, response, recovery, and mitigation activities.” The center is also directed to share information with Federal agencies and departments that have CIKR responsibilities. Information sharing is accomplished through outreach meetings with sectors, analysts, and consumers. NISAC pre-incident studies (e.g., hurricane scenario studies) are posted and available for downloading on HSIN. Selected products are reproduced for widespread dissemination in hard copy. Products requested from the NISAC program office are usually distributed by email or via electronic media.

NISAC’s objectives cover two main areas of focus:

- Provide operational support to DHS and other Federal Government entities on an as needed basis in the form of analysis, simulation, and scenario development; and
- Develop long-term capabilities by maintaining expertise in the application of analysis tools and the development of improved processes and tools in support of longer-term DHS projects.

NISAC accomplishes its mission through three types of products:

- Pre-planned, long-term analyses;
- Pre-planned, short-term analyses; and
- Unplanned, priority analytical projects that are based on higher-level tasking or that are related to current threats to CIKR (e.g., hurricane CIKR impact analysis).

Pre-planned analyses may result from several processes, but they result primarily from the National and Sector CIKR Protection Annual Reports, along with the supporting annual reports for IP, DHS' Office of Cybersecurity and Communications (CS&C), the SLTTGCC, and the RCCC. These reports identify requirements for the analyses, which are then prioritized in a similar manner to the R&D requirements.

NISAC utilizes CIKR information and data from a variety of government CIKR sector and private sector sources, including other participants in CIKR protection projects and programs. NISAC uses some data that are considered proprietary to a single industry or even to a specific firm; the data must therefore be protected from unrestricted dissemination in order to maintain the trust of the information providers. NISAC products principally serve government decisionmakers, who can derive valuable insight into incident consequences at a higher level than the supporting data could provide. In selected cases, NISAC products are made available to the private sector in order to facilitate access to key NISAC recommendations of concern to a wider community of CIKR stakeholders.

Although NISAC is the principal resource within IP for modeling, simulation, and analysis, it is not the sole source available to CIKR stakeholders in need of these capabilities. NISAC works with other stakeholders to share critical authoritative data in order to improve overall analytical quality and ensure consistency with other providers of CIKR analysis.

6.3.3 Coordination on Databases and Modeling

Integrating existing databases into DHS databases, such as the IDW, not only reduces the duplication of effort, but also ensures that available data are consistent, current, and

accurate, and provide users with a consolidated picture across all CIKR sectors. However, this approach is effective only if the source information is protected and maintained properly. Maintaining a current and useful database involves the support, coordination, and commitment of the SSAs, private sector entities, and other partners. Because the most current and accurate CIKR-related data are best known by owners and operators, the effectiveness of the effort depends on all CIKR partners keeping their databases and data systems current.

As the responsible agent for the identification of assets and existing databases for their sectors, the SSAs:

- Outline in their SSPs the sector plans and processes for database, data system, and modeling and simulation development and updates;
- Work with sector partners, as appropriate, to facilitate the collection and protection of accurate information for database, data system, and modeling and simulation use;
- Specify the timelines and milestones for the initial population of CIKR databases; and
- Specify a regular schedule for maintaining and updating the databases.

DHS works with the SSAs and other CIKR partners to:

- Identify databases and other data services that will be integrated into CIKR databases and data systems;
- Facilitate the actual integration of supporting databases or the importation of data into CIKR protection databases and data systems using a common, standardized format, data scheme, and categorization system or taxonomy specified by DHS in coordination with the SSAs; and
- Define, as appropriate, the schedule for integrating data and databases into such systems as the IDW.

6.4 Continuously Improving the NIPP and the SSPs

The NIPP uses the SCCs, GCCs, and the cross-sector councils as the primary forums for coordination of policy, planning, training, and other requirements needed to ensure efficient implementation and ongoing management and maintenance of the NIPP and the SSPs.

6.4.1 Management and Coordination

IP is the Federal executive agent for NIPP management and maintenance.

The NIPP is a multi-year plan describing mechanisms for sustaining the Nation's steady-state CIKR protection posture. The NIPP and its component SSPs include a process for: annual review; periodic interim updates as required; and regularly scheduled partial reviews and re-issuance every 3 years or more frequently, if directed by the Secretary of Homeland Security.

IP oversees the review and maintenance process for the NIPP; the SSAs, in coordination with the GCCs and SCCs, establish and operate the mechanism(s) necessary to coordinate this review for their respective SSPs. The NIPP and SSP revision processes includes developing or updating any documents necessary to carry out NIPP activities. The NIPP is reviewed at least annually to:

- Ensure that the NIPP framework is capable of measuring accomplishments in support of CIKR protection goals and objectives, and supporting the overall national approach to the homeland security mission;
- Ensure that the plan adequately reflects the organization of DHS and the SSAs;
- Ensure that the NIPP is consistent with the Federal plans and activities that it directly supports;
- Adjust practices and procedures called for in the NIPP based on changes in the national risk management environment;
- Incorporate lessons learned and best practices from day-to-day operations, exercises, and actual incidents and alerts; and
- Reflect progress in the Nation's CIKR protection, as well as changes to national priorities and guidance, critical tasks, sector organization, or national capabilities.

As changes are warranted, periodic updates to the NIPP will be issued. Types of developments that merit a periodic update include new laws, Executive Orders, Presidential directives, or regulations, and procedural changes to NIPP activities based on real-world incidents or exercise experiences.

6.4.2 Maintenance and Updates

The following paragraphs establish the procedures for posting interim changes and periodic updating of the NIPP:

- **Types of Changes:** Changes include the addition of new or supplementary material and deletions. No proposed change should contradict or override authorities or other plans contained in a statute, Executive Order, or regulation.

- **Coordination and Approval:** While DHS is the Federal executive agent for NIPP management and maintenance, any Federal department or agency with assigned responsibilities under the NIPP may propose a change to the plan. DHS is responsible for coordinating the review and approval of all proposed modifications to the NIPP with the SSAs and other CIKR partners, as appropriate. Policy changes will be coordinated and approved through the Homeland Security Council policy process.

- **Notice of Change:** DHS will issue an official Notice of Change for each interim revision to the NIPP. After publication, the modifications will be considered part of the NIPP for operational purposes pending a formal revision and re-issuance of the entire document. Interim changes can be further modified or updated using this process. (Periodic updates resulting from the annual review process do not require the formal Notice of Change.)

- **Distribution:** DHS will distribute Notices of Change to SCCs, GCCs, and other CIKR partners. Notices of Change to other organizations will be provided upon request.

- **Re-Issuance:** DHS will coordinate full reviews and updating of the NIPP every 3 years or more frequently, if directed by the Secretary of Homeland Security. The review and updating process will consider lessons learned and best practices identified during implementation in each sector and will incorporate the periodic changes and any new information technologies. DHS will distribute revised NIPP documents for interagency review and concurrence through the Homeland Security Council process.

The SSAs, in coordination with their GCCs and SCCs, establish and operate the mechanism(s) necessary to coordinate the SSP maintenance and update process in accordance with the process established for the NIPP.



7. Providing Resources for the CIKR Protection Program

Since the terrorist attacks of September 11, 2001, government and private sector expenditures to improve CIKR protection and resilience have increased across sectors and governmental jurisdictions. With finite resources available to support CIKR protection requirements, the NIPP serves as the unifying framework to ensure that CIKR investments are coordinated and address the highest priorities, based on risk, to achieve the homeland security mission and ensure the continuity of the essential infrastructure and services that support the American government, economy, and way of life. Where regulations require the use of certain tools, techniques, reporting, etc., the NIPP risk management framework is flexible enough to be implemented in a manner that supports those requirements.

This chapter describes an integrated, risk-informed approach to: guide resource support for the national CIKR protection program; focus Federal grant assistance to State, local, tribal, and territorial entities; and complement relevant private sector activities. This integrated approach coordinates CIKR protection programs and activities conducted by DHS, the SSAs, and other Federal entities through the Federal appropriations process, and focuses Federal grant funds to support national CIKR protection efforts conducted at the State, local, tribal, and territorial levels. This approach also includes mechanisms to involve private sector partners in the planning process and supports collaboration among CIKR partners to establish priorities, define requirements, share information, and maximize the use of finite resources. Implementation of this coordinated approach will help ensure that limited resources are applied efficiently and effectively to address the Nation's most critical CIKR protection needs.

7.1 The Risk-Informed Resource Allocation Process

Funding in support of CIKR protection programs at all levels is guided by a straightforward principle: Resources must be

directed to the areas of greatest priority to enable effective management of risk. By definition, all CIKR assets, systems, and networks are important. However, considering the risk factors of threat, vulnerability, and consequences, some assets, systems, networks, or functions are more critical to the Nation, as a whole, than others. This chapter describes a process to ensure that the Nation's CIKR protection resource requirements are correctly identified and appropriately prioritized to meet the most critical protection needs as well as any relevant regulatory or congressional requirements. Using a risk-informed approach, DHS collaborates with CIKR partners to identify those assets, systems, networks, and functions that are the most critical from a national perspective and lead, integrate, and coordinate a cohesive effort to help ensure their protection and resiliency. Through the NIPP framework, DHS works with the SSAs, States, and other government and private sector partners to gain an understanding of how CIKR protection is being conducted across the country, the priorities and requirements (NIPP-based or other) that drive these efforts, and how such efforts are funded. This assessment helps DHS to identify duplicative efforts and gaps across sectors and jurisdictions. DHS then uses the information gained to recommend targeted investment that helps ensure that government resources are allocated to the

areas of the greatest priority with a view toward ensuring that investments are cost-effective in reducing risk.

7.1.1 Sector-Specific Agency Reporting to DHS

Given their unique capabilities and individual risk landscapes, CIKR sectors each face different challenges. For instance, some sectors have distinct, easily identifiable assets that can be logically prioritized. Some are characterized by thousands of distributed assets, not all of which are equally critical. Others are made up of systems or networks for which the identification of specific protective measures may prove to be extremely complex, but should be attempted nonetheless. Furthermore, interdependencies among sectors can cause duplicative efforts or lead to gaps in funding for CIKR protection. To ensure that government resources are allocated according to national priorities and are based on national risk, need, and effective risk-reduction opportunities, DHS must be able to accurately assess priorities, requirements, and efforts across these diverse sectors. Requirements driven by regulations, statutes, congressional mandates, and presidential directives should also be considered.

As DHS conducts this assessment, the SSAs, supported by their respective SCCs and GCCs, provide information regarding their sectors' individual CIKR protection efforts. The SCCs participate in the process to ensure that private sector input is reflected in SSA reporting on sector priorities and requirements. The first step for an SSA in the risk-informed resource allocation process is to coordinate with sector partners, including SCCs and GCCs, as appropriate, to determine sector priorities, program requirements, and resource needs for CIKR protection. HSPD-7 requires each SSA to provide an annual report to the Secretary of Homeland Security on their efforts to identify, prioritize, and coordinate CIKR protection and resiliency in their respective sectors. Consistent with this requirement, DHS provides the SSAs with reporting guidance and templates that include requests for specific information, such as CIKR protection priorities, requirements, and resources. The following elements are included in the Sector CIKR Protection Annual Report to help inform the prioritization of resource allocation recommendations:

- Priorities and annual goals for CIKR protection and resiliency, as well as associated gaps;
- Sector-specific requirements for CIKR protection and resiliency activities and programs based on risk, need, and any other drivers such as regulations and presidential directives;
- Projected CIKR-related resource requirements for the sector, with an emphasis on anticipated gaps or shortfalls in

funding for sector- or national-level CIKR protection and resiliency; and

- CIKR, the disruption of which would cause regionally or nationally significant impacts under both steady-state and incident conditions.

7.1.2 State Government Reporting to DHS

Like sectors, State governments face diverse CIKR protection challenges and have different priorities, requirements, and available resources. Furthermore, State CIKR protection efforts are closely intertwined with those of other government and private sector partners. In particular, States work closely with local and tribal governments to address CIKR protection challenges at those levels. To accurately assess the CIKR protection effort and identify needs that warrant attention at a national level, DHS must aggregate information across State jurisdictions as it does across sectors.

DHS requires that each State develop a homeland security strategy that establishes goals and objectives for its homeland security program, which includes CIKR protection as a core element. State administrative agencies develop a Program and Capability Enhancement Plan that prioritizes statewide resource needs to support this program. The State administrative agency works with DHS to identify:

- Priorities and annual goals for CIKR protection and resiliency;
- State-specific requirements for CIKR protection activities and programs, based on risk and need;
- Mechanisms for coordinated planning and information sharing with government and private sector partners;
- CIKR, the disruption of which would cause regionally or nationally significant impacts for both steady-state and incident management purposes;
- Unfunded CIKR protection initiatives or requirements that should be considered for funding using Federal grants (described in further detail below); and
- Other funding sources utilized to implement the NIPP and address identified priorities and annual goals.

For consideration in the deliberations related to the Federal budget cycle, information on statewide CIKR resource needs must be reported to DHS by the date specified in the annual DHS Grant Programs Directorate (GPD) planning guidance. GPD includes report templates and planning guidance to support the States' reporting efforts.

7.1.3 State, Local, Tribal, and Territorial Government Coordinating Council Reporting to DHS

The intent of the SLTTGCC is to provide input and suggestions for implementation of the NIPP, including sector protection programs and initiatives. These types of engagements foster broad public sector partner involvement in actively developing CIKR protection priorities and requirements. Through the SLTTGCC Annual Report, the Council provides annual updates on CIKR programs and initiatives that are being conducted or planned by the Council, DHS, other Federal partners, or private sector partners.

7.1.4 Regional Consortium Coordinating Council Reporting to DHS

Cross-sector and multi-jurisdictional CIKR protection challenges provide an opportunity to manage interdependent risks at the regional level. Individually, the activities of the regional consortium enhance the physical security, cybersecurity, emergency preparedness, and overall public-private continuity and resiliency of one or more States, urban areas, or municipalities. The RCCC provides a unique mechanism to integrate NIPP implementation on a regional scale and details its efforts in the RCCC Annual Report.

7.1.5 Aggregating Submissions to DHS

DHS uses the information collected from the Sector CIKR Protection Annual Reports, the SLTTGCC Annual Report, the RCCC Annual Report, and State reports to assess CIKR protection status and requirements across the country. As national priorities and requirements are established, DHS will develop funding recommendations for programs and initiatives designed to reduce national-level risk in the CIKR protection mission area. In cases where gaps or duplicative efforts exist, DHS will work with the SSAs and the States to identify strategies or additional funding sources to help ensure that national CIKR protection priorities are efficiently and effectively addressed.

Following the collection, aggregation, and risk-based analysis of sector- and State-level reports, DHS summarizes this information in the National CIKR Protection Annual Report. This report details national CIKR protection priorities and requirements, and makes recommendations for prioritized focus across the Federal Government to meet national-level CIKR protection needs. The National CIKR Protection Annual Report is submitted along with the DHS budget submission to the EOP on or before September 1 as part of the annual Federal budget process (see figure 7-1).

Figure 7-1: National CIKR Protection Annual Report Process



7.2 Federal Resource Prioritization for DHS, the SSAs, and Other Federal Agencies

The Federal prioritization process described in this section is designed to ensure that the collective efforts of DHS, the SSAs, and other Federal departments and agencies support the NIPP and national priorities. It is also designed to be consistent with the DHS responsibility to coordinate overall national CIKR protection and identify national-level gaps, overlaps, or shortfalls. Driven in large part by existing and well-understood Federal budget process milestones, this approach is integrated into the established Federal budget process and reporting requirements. The process outlined in this chapter recognizes the existing budget authority and responsibilities of all Federal departments and agencies with CIKR protection-related programs and activities. We have achieved significant progress in developing a comprehensive CIKR risk management program. We will continually improve our risk management and performance measurement programs to refine their integration into the Federal budget process. The NIPP process aims to create synergy between current and future efforts to ensure a unified and effective national CIKR protection effort. The specific roles of DHS and the SSAs are described in further detail below.

7.2.1 Department of Homeland Security

DHS is responsible for overall coordination of the Nation's CIKR protection efforts. To carry out this responsibility, DHS must: identify and prioritize nationally critical assets, systems, networks, and functions; help ensure that appropriate protective initiatives are implemented; and help address any gaps or shortfalls in the protection of nationally critical CIKR. DHS works closely with the EOP to aggregate CIKR protection-related activities and related resource requests from the SSAs, other Federal departments and agencies, and other CIKR partners as a way to make informed tradeoffs in prioritizing Federal investments. These tradeoffs also consider other CIKR protection requirements that the various Federal departments and agencies must address.

DHS works with the EOP to establish a national CIKR protection strategic approach and priorities, and with the SSAs, supported by their respective SCCs and GCCs, to develop sector-specific CIKR protection-related requirements. Driven largely by the identification and prioritization of critical assets, systems, networks, and functions across sectors and States, the establishment of national protection priorities helps inform resource allocation decisions later in the process. The SSAs communicate information about their existing CIKR

protection-related programs and outstanding requirements to DHS through their Sector CIKR Protection Annual Reports. DHS uses the sector annual reports, as well as the annual reports of the SLTTGCC and the RCCC, to inform the National CIKR Protection Annual Report. The National CIKR Protection Annual Report analyzes information about sector priorities, requirements, and programs in the context of the National Risk Profile, a high-level summary of the aggregate risk and protective status of all sectors. The National Risk Profile drives the development of national priorities, which, in turn, are used to assess existing CIKR programs and to identify existing gaps or shortfalls in national CIKR protection efforts. This analysis provides the Executive Office of the President with information that supports both strategic and investment decisions related to CIKR protection and resiliency.

Figure 7-2: National CIKR Protection Annual Report Analysis



7.2.2 Sector-Specific Agencies

Earlier chapters of the NIPP articulated how DHS and the SSAs work with the respective CIKR sectors to determine risk and set priorities. Based on guidance from DHS, each SSA develops and maintains an SSP that supports the NIPP; some SSPs may also fulfill other mandates and requirements. Additionally, the SSAs, in partnership with the SCCs and GCCs, determine sector-specific priorities and requirements for CIKR protection. The SSAs submit these priorities and requirements to DHS in their sector annual reports. The SSAs work within their respective department or agency budget process to determine the CIKR protection-related aspects of their department's budget submission. SSA annual reports are submitted to DHS on or before June 1 of each year. Resource information contained in the SSA annual reports is based on appropriated funding, as well as the President's most recent budget.

Figure 7-3: DHS and SSA Roles and Responsibilities in Federal Resource Allocation

	DHS	Sector-Specific Agencies
Feb-June	<ul style="list-style-type: none"> Work with HSC to establish national NIPP priorities Through partnership mechanisms such as SCCs and GCCs, work with SSAs to develop national and sector-specific NIPP requirements 	<ul style="list-style-type: none"> Work with DHS in development of national and sector-specific NIPP requirements Develop NIPP-related aspect of budget submission with support of DHS where necessary and consistent with NIPP requirements established through collaborative process
June-Sep	<ul style="list-style-type: none"> Aggregate Annual Reports from all sectors to develop picture of national NIPP-related priorities and requirements Submit National CIKR Protection Annual Report on September 1 	<ul style="list-style-type: none"> On June 1, submit Sector CIKR Protection Annual Report to DHS that includes summary of existing NIPP-related programs
Sep-Nov	<ul style="list-style-type: none"> Work with OMB and SSAs to remedy any gaps or shortcomings in NIPP-related funding, focusing on ensuring funding of programs associated with nationally critical assets, systems, networks, or functions 	<ul style="list-style-type: none"> Work with OMB and DHS in subsequent budget deliberations to remedy any gaps or shortfalls in NIPP-related funding

Additionally, the subset of CIKR protection funding requirements directed toward R&D and S&T investments are highlighted by the SSAs, SCCs, and GCCs in the sector annual reports to inform the NCIP R&D Plan and its technology roadmap, while ensuring efficient coordination with the DHS R&D/S&T community and supporting the Federal research and technology base. These R&D and S&T plans and requirements are based on the R&D planning section of each sector’s SSP. The identified R&D requirements are prioritized based on the potential increase in CIKR protection capabilities for a given investment.

7.2.3 Summary of Roles and Responsibilities

Figure 7-3 outlines the roles and responsibilities of DHS and the SSAs throughout this process, as well as the annual timelines associated with major activities.

The final determination of funding priorities, based on the collaborative efforts of DHS, the SSAs and other Federal departments and agencies, and the EOP, guides CIKR protection programs in support of the NIPP and other applicable requirements. These priorities support Federal Government (DHS and SSA) CIKR protection activities, as well as guide and support homeland security and CIKR protection activities across and within State, local, tribal, and territorial jurisdictions.

7.3 Federal Resources for State and Local Government Preparedness

Federal grants from DHS and other Federal agencies, when available, and other programs, such as training and technical assistance, offer key support to State and local jurisdictions for CIKR protection programs. These programs provide resources to meet CIKR needs that are managed by State and local entities.

GPD is responsible for coordinating Federal homeland security grant programs to help State, local, and tribal governments enhance their ability to prevent, protect against, respond to, and recover from terrorist acts or threats and other hazards. GPD offers State, local, and tribal partners access to funding through several grant programs that can be leveraged to support CIKR protection requirements based on risk and need.

For the purposes of the NIPP, Federal grants available through DHS/GPD can be grouped into two broad categories: (1) overarching homeland security programs that provide funding for a broad set of activities in support of homeland security mission areas and the national priorities outlined in the National Preparedness Guidelines; and (2) targeted infrastructure protection programs for specific CIKR-related protection initiatives and programs within identified jurisdictions. States should leverage the range of available resources, including those from Federal, State, local, and tribal sources, as appropriate, in support of the protection activities needed to reduce vulnerabilities and close identified capability gaps related to CIKR within their jurisdictions.

7.3.1 Overarching Homeland Security Grant Programs

The overarching homeland security grant programs support activities that are conducted in accordance with the National Preparedness Guidelines. These funds support overall State and local homeland security efforts, and can be leveraged to support State, local, tribal, and/or regional CIKR protection. These funds are intended to complement and be allocated in coordination with national CIKR protection efforts.

The primary overarching homeland security grant programs include:

- **State Homeland Security Program (SHSP):** The SHSP supports the implementation of the State Homeland Security Strategy to address identified planning, organizing, equipment, training, exercise, and evaluation needs for acts of terrorism. In addition, SHSP supports the implementation of the National Preparedness Guidelines, the NIMS, the NRF, and the NIPP to support the prevention of, protection against, response to, and recovery from acts of terrorism.
- **Urban Areas Security Initiative:** UASI funds address the unique planning, organizing, equipment, training, exercise, and evaluation needs of high-threat, high-density urban areas, and assist them in building an enhanced and sustainable capacity to prevent, protect against, respond to, and recover from acts of terrorism.

7.3.2 Targeted Infrastructure Protection Programs

Targeted infrastructure protection programs include grants for specific activities that focus on the protection of CIKR, such as ports, mass transit, rail transportation, etc. These funds support CIKR protection capabilities based on risk and need in coordination with DHS, SSAs, and Federal agencies.

IP and GPD work with States to focus targeted infrastructure protection grant programs, such as the BZPP and transportation security grants, to support national-level CIKR protection priorities and to reinforce activities funded through Federal department and agency budgets and other homeland security grant programs. As appropriate, SSAs serve as subject matter experts reviewing and providing recommendations for specific target grant programs. Grantees should apply resources available under the overarching homeland security grant programs, such as SHSP and UASI, to address their regionally or locally critical CIKR protection initiatives. An additional prioritized combination of grant funding across various programs may be necessary to enable the protection of certain assets, systems, networks, and functions deemed to be nationally critical.

Available GPD grant funding is awarded to the Governor-appointed State administrative agency, which serves in each State as the lead for program implementation. Through the State administrative agencies, States will identify and prioritize their homeland security needs, including CIKR protection, and leverage assistance from these funding streams to accomplish the priorities identified in their State Homeland Security Strategies, and Program and Capability Enhancement Plans. These planning processes undertaken at the State level

are built on the common framework articulated in: the National Preparedness Guidelines; the National Priorities, including implementation of the NIPP; and capabilities enhancements based on the TCL.

DHS provides State, local, and tribal authorities with additional guidance on how to identify, assess, and prioritize CIKR protection needs and programs in support of the National Preparedness Guidelines as they apply to homeland security grants. Additional information on DHS grant programs, guidelines, allocations, and eligibility is available at: <http://www.fema.gov/grants>.

7.4 Other Federal Grant Programs That Contribute to CIKR Protection

Other Federal departments and agencies provide grant programs that can contribute to CIKR protection. These are usually sector- or threat-specific programs; many are related to technology development initiatives. Examples of these grant programs include:

- **Department of Energy:** DOE manages programs for the development of technologies to increase the resilience and reliability of the U.S. energy infrastructure. These programs address the development and demonstration of technologies and methodologies to protect physical energy infrastructure assets.
- **Department of the Interior:** The Bureau of Indian Affairs manages a grant program for the Safety of Dams on Indian Lands. Financial awards are specific to a given site; awards are restricted to Indian tribes or tribal organizations.
- **Department of Justice:** The National Institute of Justice (NIJ), Office of Justice Programs, manages a grant program for Domestic Anti-Terrorism Technology Development. The objective of the program is to support the development of counterterrorism technologies, assist in the development of standards for those technologies, and work with State and local jurisdictions to identify particular areas of vulnerability to terrorist acts and to be better prepared to respond if such acts occur. The NIJ is authorized to make grants to, or enter into contracts or cooperative agreements with, State and local governments, private nonprofit organizations, public nonprofit organizations, for-profit organizations, institutions of higher education, and qualified individuals. Applicants from the Territories of the United States and federally recognized Indian tribal governments are also eligible to participate in this program.

- **Department of Transportation:** The Pipeline and Hazardous Materials Safety Administration Pipeline Safety grant program supports efforts to develop and maintain State natural gas, liquefied natural gas, and hazardous liquid pipeline safety programs. Grant recipients are typically State government agencies.
- **Department of Transportation:** The Federal Transit Administration is a grants-in-aid agency that has several major assistance programs for eligible activities. Funds are provided through legislative formulas or discretionary authority. Funding from these programs is provided on an 80/20 Federal/local funding match basis unless otherwise specified. These assistance programs can contribute to CIKR protection efforts through funding for metropolitan and State planning and research grants; urban, non-urban, and rural transit assistance programs; bus and railway modernization efforts; major capital investments; and special flexible-funding programs.

These programs are available to a wide range of grant recipients, including CIKR owners and operators, and State, local, and tribal governments.

7.5 Setting an Agenda in Collaboration with CIKR Protection Partners

Resource allocation decisions for CIKR protection at all levels of government should align as integral components of the unified national approach established in the NIPP. In accordance with the responsibilities established in HSPD-7, DHS works with the SSAs and other government and private sector partners to set the national agenda that specifies this strategic approach to CIKR protection, articulates associated requirements, supports collaboration among partners, and recognizes the contributions of private sector partners to the overall effort. While Federal Government funding of programs and initiatives that support CIKR protection makes a significant contribution to the security of the Nation, a fully successful effort requires DHS; the SSAs; and State, local, and tribal governments to work closely with the private sector to promote the most effective use of Federal and non-Federal resources.

The NIPP uses the risk management framework to support coordination between CIKR partners outside the Federal Government. Each step of the risk management framework presents opportunities for collaboration between and among all CIKR partners. Coordination between State and local agencies and the sectors themselves ensures that cross-sector needs and priorities are more accurately identified and understood. Government coordination with private sector

owners and operators at all levels is required throughout the process to: ensure a unified national CIKR protection effort; provide accurate, secure identification of CIKR assets and systems; provide and protect risk-related information; ensure implementation of appropriate protective measures; measure program effectiveness; and make required improvements.

These opportunities for collaboration allow private sector owners and operators to benefit from CIKR protection investments in a number of ways. First, investments in CIKR protection will enable risk mitigation in a broader, all-hazards context, including common threats posed by malicious individuals or acts of nature, in addition to those posed by terrorist organizations. Second, business continuity planning can facilitate recovery of commercial activity after an incident. Finally, investing in CIKR protection within the NIPP framework will help private sector owners and operators enhance protective measures, and will support decisionmaking with more comprehensive risk-informed information. DHS explores new opportunities to encourage such collaboration through incentives (such as the SAFETY Act, which creates liability protection for sellers of qualified anti-terrorism technologies), and by providing useful information on risk assessment and management. While States typically are the eligible applicants for DHS grant programs, certain private sector entities can apply directly for grant funds through programs such as the Port Security Grant Program and the Intercity Bus Security Grant Program.

More information about the NIPP is available on the Internet at: www.dhs.gov/nipp or by contacting DHS at: nipp@dhs.gov



List of Acronyms and Abbreviations

BZPP	Buffer Zone Protection Program	FACA	Federal Advisory Committee Act
C/ACAMS	Constellation/Automated Critical Asset Management System	FBI	Federal Bureau of Investigation
CAEIAE	Centers of Academic Excellence in Information Assurance Education	FCC	Federal Communications Commission
CEO	Chief Executive Officer	FEMA	Department of Homeland Security/Federal Emergency Management Agency
CFATS	Chemical Facility Anti-Terrorism Standards	FIRST	Forum of Incident Response and Security Teams
CFDI	Critical Foreign Dependencies Initiative	FOIA	Freedom of Information Act
CFIUS	Committee on Foreign Investment in the United States	FOUO	For Official Use Only
CFR	Code of Federal Regulations	FSLC	Federal Senior Leadership Council
CII	Critical Infrastructure Information	GCC	Government Coordinating Council
CIKR	Critical Infrastructure and Key Resources	GFIRST	Government Forum of Incident Response and Security Teams
CIPAC	Critical Infrastructure Partnership Advisory Council	GPD	FEMA/Grant Programs Directorate (Division of DHS Preparedness Directorate)
CWIN	Critical Infrastructure Warning Information Network	GPS	Global Positioning System
COG	Continuity of Government	GSA	General Services Administration
COI	Community of Interest	HHS	Department of Health and Human Services
COOP	Continuity of Operations	HITRAC	Department of Homeland Security's Homeland Infrastructure Threat and Risk Analysis Center
COP	Common Operating Picture	HMGP	Hazard Mitigation Grant Program
CSIA IWG	Cyber Security and Information Assurance Interagency Working Group	HSAC	Homeland Security Advisory Council
CSIRT	Computer Security Incident Response Teams	HSAS	Homeland Security Advisory System
DHS	Department of Homeland Security	HSC	Homeland Security Council
DoD	Department of Defense	HSEEP	Homeland Security Exercise and Evaluation Program
DOE	Department of Energy	HSIN	Homeland Security Information Network
DOJ	Department of Justice	HSIN-CS	Homeland Security Information Network for Critical Sectors
DOT	Department of Transportation	HSIP	Homeland Security Infrastructure Program
ECTF	Electronic Crimes Task Force	HSOC	Homeland Security Operations Center
E.O.	Executive Order	HSPD	Homeland Security Presidential Directive
EOP	Executive Office of the President	iCAV	Integrated Common Analytical Viewer
EPA	Environmental Protection Agency		

IDW	Infrastructure Data Warehouse	NICC	National Infrastructure Coordinating Center
IED	Improvised Explosive Device	NIJ	National Institute of Justice
IICD	Infrastructure Information Collection Division	NIMS	National Incident Management System
IICP	Infrastructure Information Collection Program	NIPP	National Infrastructure Protection Plan
IICS	Infrastructure Information Collection System	NISAC	National Infrastructure Simulation and Analysis Center
IICV	Infrastructure Information Collection and Visualization	NIST	National Institute of Standards and Technology
IDM	Infrastructure Data Management	NJTTF	National Joint Terrorism Task Force
IP	Office of Infrastructure Protection (Division of DHS National Protection and Programs Directorate)	NOC	National Operations Center
IRAPP	Infrastructure Risk Analysis Partnership Program	NOC-HQE	National Operations Center—Headquarters Element
ISAC	Information Sharing and Analysis Center	NRC	Nuclear Regulatory Commission
ISE	Information-Sharing Environment	NRCC	National Response Coordination Center
IWWN	International Watch and Warning Network	NRF	National Response Framework
IV	Infrastructure Visualization	NSA	National Security Agency
JCG	Joint Contact Group	NSC	National Security Council
JTTF	Joint Terrorism Task Force	NS/EP	National Security and Emergency Preparedness
LEO	Law Enforcement Online	NSTAC	National Security Telecommunications Advisory Committee
MIFC	Maritime Intelligence Fusion Center	NSTC	National Science and Technology Council
MS-ISAC	Multi-State Information Sharing and Analysis Center	OAS	Organization of American States
NATO	North Atlantic Treaty Organization	OCA	Original Classification Authority
NCC	National Coordinating Center for Telecommunications	OECD	Organisation for Economic Co-operation and Development
NCIP R&D	National Critical Infrastructure Protection Research and Development	OI&A	Office of Intelligence and Analysis (Division of DHS Preparedness Directorate)
NCRCG	National Cyber Response Coordination Group	OMB	Office of Management and Budget
NCS	National Communications System	OSTP	Office of Science and Technology Policy
NCSA	National Cyber Security Alliance	PCC	Policy Coordination Committee
NCSD	DHS National Cyber Security Division	PCII	Protected Critical Infrastructure Information
NCTC	National Counterterrorism Center	PDD	Presidential Decision Directive
NEP	National Exercise Program	PNT	Position, Navigation, and Timing
NHC	National Hurricane Center	PSA	Protective Security Advisor
NIAC	National Infrastructure Advisory Council	PVTSAC	Private Sector Senior Advisory Committee
NIAP	National Information Assurance Partnership	RCCC	Regional Consortium Coordinating Council
		R&D	Research and Development
		RISS	Regional Information Sharing Systems

SAV	Site Assistance Visit
SCADA	Supervisory Control and Data Acquisition
SCC	Sector Coordinating Council
SHIRA	Strategic Homeland Infrastructure Risk Analysis
SHSP	State Homeland Security Program
SLFC	State and Local Fusion Center
SLTTGCC	State, Local, Tribal, and Territorial Government Coordinating Council
SPP	Security and Prosperity Partnership of North America
SSA	Sector-Specific Agency
SSI	Sensitive Security Information
SSP	Sector-Specific Plan
S&T	Science and Technology Directorate of DHS
SVA	Security Vulnerability Assessment
TCL	Target Capabilities List
TSA	Transportation Security Administration
UASI	Urban Areas Security Initiative
UCNI	Unclassified Controlled Nuclear Information
UDOP	User Defined Operational Picture
U.S.	United States
U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team
USCG	United States Coast Guard
UTL	Universal Task List
VBIED	Vehicle Borne Improvised Explosive Device
VISAT	Vulnerability Identification Self-Assessment Tool
WMD	Weapons of Mass Destruction



Glossary of Key Terms

Many of the definitions in this Glossary are derived from language enacted in Federal laws and/or included in national plans, including the Homeland Security Act of 2002, the USA PATRIOT Act of 2001, the National Incident Management System, and the National Response Framework. Additional definitions come from the DHS Lexicon.

All-Hazards. A grouping classification encompassing all conditions, environmental or manmade, that have the potential to cause injury, illness, or death; damage to or loss of equipment, infrastructure services, or property; or alternatively causing functional degradation to social, economic, or environmental aspects.

Asset. Person, structure, facility, information, material, or process that has value. In the context of the NIPP, people are not considered assets.

Business Continuity. The ability of an organization to continue to function before, during, and after a disaster.

Chemical Facility Anti-Terrorism Standards (CFATS). Section 550 of the DHS Appropriations Act of 2007 grants the Department of Homeland Security the authority to regulate chemical facilities that “present high levels of security risk.” The CFATS establish a risk-informed approach to screening and securing chemical facilities determined by DHS to be “high risk.”

CIKR Partner. Those Federal, State, local, tribal, or territorial governmental entities, public and private sector owners and operators and representative organizations, regional organizations and coalitions, academic and professional entities, and certain not-for-profit and private volunteer organizations that share in the responsibility for protecting the Nation’s CIKR.

Consequence. The effect of an event, incident, or occurrence. For the purposes of the NIPP, consequences are divided into four main categories: public health and safety, economic, psychological, and governance impacts.

Control Systems. Computer-based systems used within many infrastructure and industries to monitor and control sensitive processes and physical functions. These systems typically collect measurement and operational data from the field, process and display the information, and relay control commands to local or remote equipment or human-machine interfaces

(operators). Examples of types of control systems include SCADA systems, Process Control Systems, and Distributed Control Systems.

Critical Infrastructure. Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction.

Critical Infrastructure Information (CII). Information that is not customarily in the public domain and is related to the security of critical infrastructure or protected systems. CII consists of records and information concerning any of the following:

- Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law; harms the interstate commerce of the United States; or threatens public health or safety.
- The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit.
- Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, insurance, or continuity, to the extent that it is related to such interference, compromise, or incapacitation.

Cybersecurity. The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. Includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems.

Cyber System. Any combination of facilities, equipment, personnel, procedures, and communications integrated to provides cyber services. Examples include business systems, control systems, and access control systems.

Dependency. The one-directional reliance of an asset, system, network, or collection thereof, within or across sectors, on input, interaction, or other requirement from other sources in order to function properly.

Function. Service, process, capability, or operation performed by an asset, system, network, or organization.

Government Coordinating Council. The government counterpart to the SCC for each sector established to enable interagency coordination. The GCC comprises representatives across various levels of government (Federal, State, local, tribal, and territorial) as appropriate to the security and operational landscape of each individual sector.

Hazard. Natural or manmade source or cause of harm or difficulty.

HSPD-19. This directive establishes a national policy and calls for the development of a national strategy and implementation plan on the prevention and detection of, protection against, and response to terrorist use of explosives in the United States.

Incident. An occurrence, caused by either human action or natural phenomena, that may cause harm and may require action. Incidents can include major disasters, emergencies, terrorist attacks, terrorist threats, wild and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, and other occurrences requiring an emergency response.

Infrastructure. The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole. Consistent with the definition in the Homeland Security Act, infrastructure includes physical, cyber, and/or human elements.

Interdependency. Mutually reliant relationship between entities (objects, individuals, or groups). The degree of interdependency does not need to be equal in both directions.

Key Resources. As defined in the Homeland Security Act, key resources are publicly or privately controlled resources

essential to the minimal operations of the economy and government.

Mitigation. Ongoing and sustained action to reduce the probability of or lessen the impact of an adverse incident.

Network. A group of components that share information or interact with each other in order to perform a function.

Normalize. In the context of the NIPP, the process of transforming risk-related data into comparable units.

Owners/Operators. Those entities responsible for day-to-day operation and investment in a particular asset or system.

Preparedness. Activities necessary to build, sustain, and improve readiness capabilities to prevent, protect against, respond to, and recover from natural or manmade incidents. Preparedness is a continuous process involving efforts at all levels of government and between government and the private sector and nongovernmental organizations to identify threats, determine vulnerabilities, and identify required resources to prevent, respond to, and recover from major incidents.

Prevention. Actions taken and measures put in place for the continual assessment and readiness of necessary actions to reduce the risk of threats and vulnerabilities, to intervene and stop an occurrence, or to mitigate effects.

Prioritization. In the context of the NIPP, prioritization is the process of using risk assessment results to identify where risk-reduction or -mitigation efforts are most needed and subsequently determine which protective actions should be instituted in order to have the greatest effect.

Protected Critical Infrastructure Information (PCII). PCII refers to all critical infrastructure information, including categorical inclusion PCII, that has undergone the validation process and that the PCII Program Office has determined qualifies for protection under the CII Act. All information submitted to the PCII Program Office or Designee with an express statement is presumed to be PCII until the PCII Program Office determines otherwise.

Protection. Actions or measures taken to cover or shield from exposure, injury, or destruction. In the context of the NIPP, protection includes actions to deter the threat, mitigate the vulnerabilities, or minimize the consequences associated with a terrorist attack or other incident. Protection can include a wide range of activities, such as hardening facilities, building resiliency and redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing security systems, promoting

workforce surety, training and exercises, and implementing cybersecurity measures, among various others.

Recovery. The development, coordination, and execution of service- and site-restoration plans for affected communities and the reconstitution of government operations and services through individual, private sector, nongovernmental, and public assistance programs that identify needs and define resources; provide housing and promote restoration; address long-term care and treatment of affected persons; implement additional measures for community restoration; incorporate mitigation measures and techniques, as feasible; evaluate the incident to identify lessons learned; and develop initiatives to mitigate the effects of future incidents.

Resilience. The ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions.

Response. Activities that address the short-term, direct effects of an incident, including immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution of emergency operations plans and incident mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increasing security operations; continuing investigations into the nature and source of the threat; ongoing surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at preempting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.

Risk. The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.

Risk-Informed Decisionmaking. The determination of a course of action predicated on the assessment of risk, the expected impact of that course of action on that risk, and other relevant factors.

Risk Management Framework. A planning methodology that outlines the process for setting goals and objectives; identifying assets, systems, and networks; assessing risks; prioritizing and implementing protection programs and resiliency strategies; measuring performance; and taking corrective action. Public and private sector entities often include risk management frameworks in their business continuity plans.

Sector. A logical collection of assets, systems, or networks that provide a common function to the economy, govern-

ment, or society. The NIPP addresses 18 CIKR sectors, identified by the criteria set forth in HSPD-7.

Sector Coordinating Council. The private sector counterpart to the GCC, these councils are self-organized, self-run, and self-governed organizations that are representative of a spectrum of key stakeholders within a sector. SCCs serve as the government's principal point of entry into each sector for developing and coordinating a wide range of CIKR protection activities and issues.

Sector Partnership Model. The framework used to promote and facilitate sector and cross-sector planning, coordination, collaboration, and information sharing for CIKR protection involving all levels of government and private sector entities.

Sector Specialists. DHS Sector Specialists provide coordination and integration capability across the CIKR sectors to provide senior DHS decisionmakers with strategic (national-level) situational awareness and assessments of CIKR impacts both on a steady-state basis and during incidents.

Sector-Specific Agency. Federal departments and agencies identified in HSPD-7 as responsible for CIKR protection activities in specified CIKR sectors.

Sector-Specific Plan. Augmenting plans that complement and extend the NIPP Base Plan and detail the application of the NIPP framework specific to each CIKR sector. SSPs are developed by the SSAs in close collaboration with other sector partners.

Steady-State. In the context of the NIPP, steady-state is the posture for routine, normal, day-to-day operations as contrasted with temporary periods of heightened alert or real-time response to threats or incidents.

System. Any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose.

Terrorism. Premeditated threat or act of violence against non-combatant persons, property, and environmental or economic targets to induce fear, intimidate, coerce, or affect a government, the civilian population, or any segment thereof, in furtherance of political, social, ideological, or religious objectives.

Threat. A natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.

Tier 1. Tier 1 facilities and systems are those that if successfully destroyed or disrupted through terrorist attack would cause major national or regional impacts similar to those

experienced with Hurricane Katrina or the September 11, 2001, attacks.

Tier 2. Tier 2 facilities and systems are those that meet predefined, sector-specific criteria and that are not Tier 1 facilities or systems.

Value Proposition. A statement that outlines the national and homeland security interest in protecting the Nation's CIKR and articulates the benefits gained by all CIKR partners through the risk management framework and public-private partnership described in the NIPP.

Vulnerability. A physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.

Weapons of Mass Destruction. Weapon capable of a high order of destruction and/or of being used in such a manner as to destroy large numbers of people or an amount of property.

Appendix 1: Special Considerations

Appendix 1A: Cross-Sector Cybersecurity

1A.1 Introduction

The United States relies on cyber infrastructure for government operations, a vibrant economy, and the health and safety of its citizens. However, malicious actors can and do conduct attacks against critical cyber infrastructure on an ongoing basis. While both public and private sector owners and operators actively manage the risk to their operations through monitoring and mitigation activities designed to prevent daily incidents from becoming significant disruptions, increasingly sophisticated threats require a more thorough examination of cyber risk and the associated risks to cybersecurity. Furthermore, nation-states are realizing that hacking tools, methods, and tactics offer asymmetric opportunities for espionage, countering military force, and economic and geopolitical advantages. These threat vectors, combined with insider threat and a range of other pervasive cyber threats to critical infrastructure, highlight the need for public, private, academic, and international entities to collaborate and enhance cybersecurity awareness and preparedness efforts, and to ensure that the cyber elements of CIKR are:

- Robust enough to withstand attacks without incurring catastrophic damage;
- Resilient enough to sustain nationally critical operations; and
- Responsive enough to recover from attacks in a timely manner.

While Chapter 3 of the NIPP discusses specific cybersecurity concerns during each phase of the NIPP risk management framework, the following sections of this appendix discuss the processes, procedures, tools, programs, and methodologies that public and private sector entities, CIKR sectors, academic institutions, and international entities can use to enhance cybersecurity.

1A.1.1 Value Proposition for Cybersecurity

The value proposition for cybersecurity aligns with that for CIKR protection in general, as discussed in chapter 1 of the NIPP, but with a concentrated focus on cyber infrastructure. Many CIKR functions and services are enabled through cyber systems

and services; if cybersecurity is not appropriately addressed, the risk to CIKR is increased. The responsibility for cybersecurity spans all CIKR partners, including public and private sector entities. The NIPP provides a coordinated and collaborative approach to help public and private sector partners understand and manage cyber risk.

The NIPP promotes cybersecurity by facilitating participation and partnership in CIKR protection initiatives, leveraging cyber-specific expertise and experiences, and improving information exchange and awareness of cybersecurity concerns. It also provides a framework for public and private sector partner efforts to recognize and address the similarities and differences among the approaches to cyber risk management for business continuity and national security. This framework enables CIKR partners to work collaboratively to make informed cyber risk management decisions, define national cyber priorities, and address cybersecurity as part of an overall national CIKR protection strategy.

1A.1.2 Definitions

The following definitions explain key terms and concepts related to the cyber dimension of CIKR protection:

- **Cyber Infrastructure:** Includes electronic information and communications systems and services and the information contained therein. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information. For example: computer systems; control systems (e.g., SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) are part of cyber infrastructure:
 - Producers and providers of cyber infrastructure and services represent the information technology industrial base and make up the Information Technology Sector. The producers and providers of cyber infrastructure and services play a key role in developing secure and reliable products and services.
 - Consumers of cyber infrastructure must maintain its security as new vulnerabilities are identified and the threat environment evolves. Individuals, whether private citizens or employees with cyber systems administration responsibility, play a significant role in managing the security of computer systems to ensure that they are not used to enable attacks against CIKR.
- **Information Technology (IT):** These critical functions are sets of processes that produce, provide, and maintain products and services. IT critical functions encompass the full set of processes (e.g., R&D, manufacturing, distribution, upgrades, and maintenance) involved in transforming supply inputs to IT products and services.
- **Cybersecurity:** The prevention of damage to, unauthorized use of, exploitation of, and, if needed, the restoration of electronic information and communications systems and services (and the information contained therein) to ensure confidentiality, integrity, and availability.
- **Cross-Sector Cybersecurity:** Collaborative efforts among DHS, the SSAs, and other CIKR partners to improve the cybersecurity of the CIKR sectors by facilitating cyber risk-mitigation activities.

1A.1.3 Cyber-Specific Authorities

Various Federal strategies, directives, policies, and regulations provide the basis for Federal actions and activities associated with implementing the cyber-specific aspects of the NIPP. The four primary authorities associated with cybersecurity are the National Strategy to Secure Cyberspace, HSPD-7, NSPD-54/HSPD-23, and the Homeland Security Act. These documents are described in further detail in appendix 2A.

1A.2 Cybersecurity Responsibilities

The National Strategy to Secure Cyberspace, HSPD-7, NSPD-54/HSPD-23, and the Homeland Security Act identify the responsibilities of the various CIKR partners with a role in securing cyberspace. These roles and responsibilities are described in more detail below.

1A.2.1 Department of Homeland Security

In accordance with HSPD-7, DHS is a principal focal point for the security of cyberspace. DHS has specific responsibilities regarding the coordination of the efforts of CIKR partners to prevent damage, unauthorized use, and exploitation and to enable the restoration of cyber infrastructure to ensure confidentiality, integrity, and availability. These responsibilities include:

- Developing a comprehensive national plan for securing U.S. CIKR;
- Providing crisis management in response to incidents involving cyber infrastructure;
- Providing technical assistance to other governmental entities and the private sector with respect to emergency recovery plans for incidents involving cyber infrastructure;
- Coordinating with other Federal agencies to provide specific warning information and advice on appropriate protective measures and countermeasures to: State, local, and tribal governments; the private sector; academia; and the public;
- Conducting and funding cybersecurity R&D, in partnership with other agencies, which will lead to new scientific understanding and technologies in support of homeland security; and
- Assisting the SSAs in understanding and mitigating cyber risk, and in developing effective and appropriate protective measures.

Within the risk management framework described in the NIPP, DHS is also responsible for the following activities:

- Providing cyber-specific expertise and assistance in addressing the cyber elements of CIKR;
- Promoting a comprehensive national awareness program to empower businesses, the workforce, and individuals to secure their own segments of cyberspace;
- Working with CIKR partners to reduce cyber vulnerabilities and minimize the severity of cyber attacks;
- Coordinating the development and conduct of national cyber threat assessments;
- Providing input on cyber-related issues for the National Intelligence Estimate of cyber threats to the United States;
- Facilitating cross-sector cyber analysis to understand and mitigate cyber risk;
- Providing guidance, review, and functional advice on the development of effective cyber-protective measures; and
- Coordinating cybersecurity programs and contingency plans, including the recovery of Internet functions.

1A.2.2 Sector-Specific Agencies

Recognizing that each CIKR sector possesses its own unique characteristics and operating models, the SSAs provide subject matter and industry expertise through relationships with the private sector to enable protection of the assets, systems, networks, and functions that they provide within each of the sectors. The SSAs are working with their private sector counterparts to understand and mitigate cyber risk by:

- Identifying subject matter expertise regarding the cyber aspects of their sector;
- Increasing awareness of how the business and operational aspects of the sector rely on cyber systems and processes;
- Determining whether approaches for CIKR inventory, risk assessment, and protective measures currently: address cyber assets, systems, and networks; require enhancement; or require the use of alternative approaches;
- Reviewing and modifying existing and future sector efforts to ensure that cyber concerns are fully integrated into sector security strategies and protective activities;
- Establishing mutual assistance programs for cybersecurity emergencies, as appropriate;
- Establishing planning, training, and exercise programs according to HSEEP; and

- Exchanging cyber-specific information with sector partners, including the international community, as appropriate, to improve the Nation's overall cybersecurity posture.

1A.2.3 Other Federal Departments and Agencies

All Federal departments and agencies must manage the security of their cyber infrastructure while maintaining an awareness of vulnerabilities and consequences to ensure that the cyber infrastructure is not used to enable attacks against the Nation's CIKR. A number of Federal agencies have specific additional responsibilities outlined in the National Strategy to Secure Cyberspace:

- **The Department of Justice and the Federal Trade Commission:** Working with the sectors to address barriers to mutual assistance programs for cybersecurity emergencies.
- **The Department of Justice and Other Federal Agencies:**
 - Developing and implementing efforts to reduce or mitigate cyber threats by acquiring more robust data on victims of cyber crime and intrusions;
 - Leading the national effort to investigate and prosecute those who conduct or attempt to conduct cyber attacks;
 - Exploring the means to provide sufficient investigative and forensic resources and training to facilitate expeditious investigation and resolution of CIKR incidents; and
 - Identifying ways to improve cyber information sharing and investigative coordination among Federal, State, local, and tribal law enforcement communities; other agencies; and the private sector.
- **The Federal Bureau of Investigation and the Intelligence Community:** Ensuring a strong counterintelligence posture to deter intelligence collection against the Federal Government, as well as commercial and educational organizations.
- **The Intelligence Community, the Department of Defense, and Law Enforcement Agencies:** Improving the Nation's ability to quickly attribute the source of threats or attacks to enable a timely and effective response.

1A.2.4 State, Local, Tribal, and Territorial Governments

State, local, tribal, and territorial governments are encouraged to implement the following cyber recommendations:

- Managing the security of their cyber infrastructure while maintaining an awareness of threats, vulnerabilities, and consequences to ensure that it is not used to enable attacks against CIKR, and ensuring that government offices manage their computer systems accordingly;
- Participating in significant national, regional, and local awareness programs to encourage local governments and citizens to manage their cyber infrastructure appropriately;
- Establishing planning, training, and exercise programs according to HSEEP; and
- Establishing cybersecurity programs, including policies, plans, procedures, recognized business practices, awareness, and audits.

1A.2.5 Owners and Operators

Owners and operators are encouraged to implement the following recommendations as indicated in the National Strategy to Secure Cyberspace:

- Managing the security and resiliency of their cyber infrastructure while maintaining an awareness of vulnerabilities and consequences to ensure that it is not used to enable attacks against the Nation's CIKR;
- Participating in sector-wide programs to share information on cybersecurity;
- Evaluating the security of networks that affect the security of the Nation's CIKR, including:

- Conducting audits to ensure effectiveness and the use of best practices;
- Developing continuity plans that consider the full spectrum of necessary resources, including off-site staff and equipment; and
- Participating in industry-wide information sharing and best practices dissemination;
- Reviewing and exercising continuity plans for cyber infrastructure and examining alternatives (e.g., diversity in service providers, implementation of recognized cybersecurity practices) as a way of improving resiliency and mitigating risk;
- Identifying near-term R&D priorities that include programs for highly secure and trustworthy hardware, software, and protocols; and
- Promoting more secure out-of-the-box installation and implementation of software industry products, including: increasing user awareness of the security features of products; ease of use for security functions; and, where feasible, promotion of industry guidelines and best practices that support such efforts.

1A.2.6 Academia

Colleges and universities are encouraged to implement several recommendations as indicated in the National Strategy to Secure Cyberspace:

- Managing the security of their cyber infrastructure while maintaining awareness of vulnerabilities and consequences to ensure that it is not used to enable attacks against the Nation’s CIKR;
- Establishing appropriate information-sharing mechanisms to deal with cyber attacks and vulnerabilities;
- Establishing an on-call point of contact for Internet service providers and law enforcement officials in the event that the institution’s cyber assets, systems, or networks are discovered to be launching cyber attacks; and
- Establishing model guidelines empowering Chief Information Officers to manage cybersecurity, develop and exchange best practices for cybersecurity, and promote model user awareness programs.

1A.3 Cross-Sector Cybersecurity Programs

Since each sector has a unique reliance on cyber infrastructure, DHS will assist the SSAs in developing a range of effective and appropriate cyber-protective measures. To assist the SSAs, DHS has established several vulnerability-reduction programs under the NIPP risk management framework, including:

- **Critical Infrastructure Protection Cybersecurity (CIP CS) Program:** The CIP CS Program strengthens preparedness by partnering with the public and private sectors to improve the security of the IT Sector and cybersecurity across the Nation’s critical infrastructure by facilitating risk management activities that reduce cyber vulnerabilities and minimize the severity of cyber attacks. The program includes responsibility for the development and implementation of the IT SSP; for cross-sector cyber support to SSAs as they maintain and implement their SSPs and reduce cyber risk to their sectors; and support to IP for development of the NIPP’s cyber component, SSP development guidance and technical assistance sessions, and the National CIKR Protection Annual Report.
- **Software Assurance Program:** Public and private sector partners work together to develop best practices and new technologies to promote integrity, security, and reliability in software development. DHS leads the Software Assurance Program, a comprehensive effort that addresses people,

Cyber Security Vulnerability Assessment (CSVA)

Developed by the DHS National Cyber Security Division (NCSD) CIP CS Program, the CSVA is a flexible and scalable approach that analyzes an entity’s cybersecurity posture and describes gaps and targeted considerations that can reduce overall cyber risks.

The CSVA assesses the policies, plans, and procedures in place to reduce cyber vulnerabilities and leverages various recognized standards, guidance, and methodologies (e.g., International Organization for Standardization 27001, Information Systems Audit and Control Association (ISACA) Control Objects for Information and Related Technologies (COBIT), and the NIST Special Publication 800 series).

processes, technology, and acquisition throughout the software life cycle. Focused on shifting away from the current security paradigm of patch management, these efforts will encourage the production of higher quality, more secure software. These efforts to promote a broader ability to routinely develop and deploy trustworthy software products through public-private partnerships are a significant element of securing cyberspace and the Nation's CIKR. DHS also partners with NIST in the National Information Assurance Partnership (NIAP), a Federal Government initiative originated to meet the security testing needs of both information technology consumers and producers. NIAP is operated by NSA to address security testing, evaluation, and validation programs.

- **Control System Security Program:** The NCSO Control System Security Program coordinates efforts among Federal, State, local, tribal, and territorial governments, as well as control system owners, operators, and vendors to improve control system security within and across all CIKR sectors. The Control System Security Program coordinates activities to reduce the likelihood of the success and severity of a cyber attack against critical infrastructure control systems through risk-mitigation activities. These activities include assessing and managing control system vulnerabilities, assisting the US-CERT Control Systems Security Center with control system incident management, and providing control system situational awareness through outreach and training initiatives.

Control System Cyber Security Self-Assessment Tool (CS2SAT)

Developed by the NCSO Control System Security Program, the CS2SAT is a desktop software tool that guides users through a step-by-step process to assess their control system network and then makes appropriate recommendations for improving the system's cybersecurity posture based on recognized security standards.

The tool derives its recommendations from a database of cybersecurity practices that have been adapted specifically for application to industry control system networks and components.

Each recommendation is linked to a set of actions that can be applied to remediate specific security vulnerabilities.

- **The Standards and Best Practices Program:** As part of its efforts to develop practical guidance and review tools, and to promote R&D investment in cybersecurity, DHS and NIST co-sponsor the National Vulnerability Database. This database provides centralized and comprehensive vulnerability mitigation resources for all types of users, including the general public, system administrators, and vendors to assist with incident prevention and management (including links to patches) to mitigate consequences and vulnerabilities.
- **The Cyber Exercise Program:** Through this program, DHS and CIKR partners conduct exercises to improve coordination among members of the cyber incident response community, including Federal, State, local, tribal, territorial, and international governmental entities, as well as private sector corporations, coordinating councils, and academic institutions. The main objectives of national cyber exercises are to: practice coordinated response to cyber attack scenarios; provide an environment for evaluation of interagency and cross-sector processes, procedures, and tools for communications and response to cyber incidents; and foster improved information sharing among government agencies and between government and private industry.

In addition to specific DHS cybersecurity infrastructure protection programs, DHS has partnered with other public and private sector entities to develop and implement specific programs to help improve the security of cyber infrastructure across sectors, as well as to support national cyber risk-mitigation activities, including:

- **Government Forum of Incident Response and Security Teams (GFIRST):** Following the model of the global FIRST organization, the Federal interagency community established GFIRST to facilitate interagency information sharing and cooperation across Federal agencies for readiness and response efforts. GFIRST is a group of technical and tactical security response team practitioners who are responsible for securing government IT systems. The members work together to understand and deal with computer security incidents and to encourage proactive and preventive security practices.
- **Cross-Sector Cybersecurity Working Group (CSCSWG):** The CSCSWG serves as a forum to bring government and the private sector together to collaboratively address risk across the CIKR sectors. This cross-sector perspective facilitates the sharing of perspectives and knowledge about various cybersecurity concerns, such as common vulnerabilities and protective measures, and leverages functional cyber expertise in a comprehensive forum.
- **The National Cyber Response Coordination Group (NCRCG):** The NCRCG serves as the Federal Government's principal interagency mechanism for operational information sharing and coordination of Federal Government response and recovery efforts during a cyber crisis. NCRCG member agencies use their established relationships with the private sector and State,

local, tribal, and territorial governments to facilitate cyber incident management, develop courses of action, and devise appropriate response and recovery strategies. NCRCG facilitates coordination of the Federal Government's efforts to prepare for, respond to, and recover from cyber incidents and physical attacks that have significant cyber consequences.

The Federal Government is continually increasing their capability to address cyber risk associated with critical networks and information systems beyond the previously mentioned DHS and DHS-partnered programs and entities. NSPD-54/HSPD-23 outlined the Comprehensive National Cybersecurity Initiative (CNCI) and a series of continuous efforts designed to establish a frontline defense by: reducing current vulnerabilities and preventing intrusions; defending against the full spectrum of threats by using intelligence and strengthening supply chain security; and shaping the future environment by enhancing our research, development, and education, as well as investing in leap-ahead technologies.

NSPD-54/HSPD-23 directs the Secretary of Homeland Security, in consultation with the heads of other SSAs, to submit a report detailing the policy and resource requirements for improving the protection of privately owned U.S. CIKR networks. The report details how the Federal Government can partner with the private sector to leverage investment in technology, increase awareness about the extent and severity of the cyber threats facing CIKR, and enhance real-time cyber situational awareness. Under the auspices of the CIPAC, DHS formed a private sector CIKR working group to respond to this task. Private sector input proved to be critical in enabling DHS to fully appreciate the scale and scope of the task and to develop a set of actionable recommendations that accurately reflect the reality of the shared responsibility between the public and private sectors with respect to securing the Nation's cyber assets, systems, and networks. DHS is now working through the CIPAC and NIPP Partnership Framework to implement the short- and long-term recommendations in the report, as well as engage the private sector in other CNCI activities.

1A.4 Ensuring Long-Term Cybersecurity

The effort to ensure a coherent cyber CIKR protection program over the long term has four components that are described in greater detail below:

- **Information Sharing and Awareness:** Ensures implementation of effective, coordinated, and integrated protection of cyber assets, systems, and networks, and the functions that they provide, and enables cybersecurity partners to make informed decisions with regard to short- and long-term cybersecurity postures, risk mitigation, and operational continuity.
- **International Cooperation:** Promotes a global culture of cybersecurity and improves the overall cyber incident preparedness and response posture.
- **Training and Education:** Ensures that skilled and knowledgeable cybersecurity professionals are available to undertake NIPP programs in the future.
- **Research and Development:** Improves cybersecurity protective capabilities or dramatically lowers the costs of existing capabilities so that State, local, tribal, territorial, and private sector partners can afford to do more with their limited budgets.

1A.4.1 Information Sharing and Awareness

Information sharing and awareness involves sharing programs with agency partners and other CIKR partners, and special sharing arrangements for emergency situations. Each of these is discussed below:

Interagency Coordination: Interagency cooperation and information sharing are essential to improving national cyber counterintelligence and law enforcement capabilities. The intelligence and law enforcement communities have both official and informal mechanisms in place for information sharing that DHS supports:

- FBI's Cyber Task Forces involve more than 50 law enforcement agency cyber task forces and more than 80 additional cyber working groups throughout the country, collaborating with Federal, State, and local partners to maximize investigative resources to ensure a timely and effective response to cybersecurity threats of both a criminal and a national security nature.
- FBI's InfraGard program is a public-private partnership coordinated out of the 56 FBI field offices nationwide. This program brings together law enforcement, academia, and private sector entities on a monthly basis to provide a forum for information sharing and networking.

- FBI's Inter-Agency Coordination Cell is a multi-agency group focused on sharing law enforcement information on cyber-related investigations.
- U.S. Secret Service's Electronic Crimes Task Forces provide interagency coordination on cyber-based attacks and intrusions.

Information Sharing and Analysis Centers: Underscoring the effectiveness of cybersecurity efforts is the importance of information sharing between and among industry and government. To this end, the Information Technology and Communications ISACs work closely together and with DHS and the SSAs to maximize resources, coordinate preparedness and response efforts, and maintain situational awareness to enable risk mitigation regarding cyber infrastructure.

Cybersecurity Awareness for CIKR Partners: DHS plays an important leadership role in coordinating a public-private partnership to promote and raise cybersecurity awareness among the general public by:

- Partnering with other Federal and private sector organizations to sponsor the National Cyber Security Alliance (NCSA), including creating a public-private organization, Stay Safe Online, to educate home users, small businesses, and K-12 and higher education audiences on cybersecurity best practices.
- Engaging with the MS-ISAC to help enhance the Nation's cybersecurity readiness and response at the State and local levels, and launching a national cybersecurity awareness effort in partnership with the MS-ISAC. The MS-ISAC is an information-sharing organization, with representatives of State and local governments, that analyzes, sanitizes, and disseminates information pertaining to cyber events and vulnerabilities to its constituents and private industry.
- Collaborating with the NCSA, the MS-ISAC, and the public and private sector to establish October as National Cyber Security Awareness Month and participating in activities to continuously raise cybersecurity awareness nationwide.

Cyberspace Emergency Readiness: DHS established the US-CERT, which is a 24/7 single point of contact for cyberspace analysis and warning, information sharing, and incident response and recovery for a broad range of users, including government, enterprises, small businesses, and home users. US-CERT is a partnership between DHS and the public and private sectors that is designed to help secure the Nation's Internet infrastructure and coordinate defenses against and responses to cyber attacks across the Nation. US-CERT is responsible for:

- Analyzing and reducing cyber threats and vulnerabilities;
- Disseminating cyber threat warning information; and
- Coordinating cyber incident response activities.

To support the information-sharing requirements of the network approach, US-CERT provides the following information on their Web site, which is accessible through the HSIN and by mail:

- **Cybersecurity Alerts:** Written in a language for home, corporate, and new users, these alerts are published in conjunction with technical alerts in the context of security issues that affect the general public.
- **Cybersecurity Bulletins:** Bulletins summarize information that has been published regarding emergent security issues and vulnerabilities. They are published weekly and are written primarily for systems administrators and other technical users.
- **Cybersecurity Tips:** Tips provide information and advice on a variety of common cybersecurity topics. They are published biweekly and are written primarily for home, corporate, and new users.
- **National Web Cast Initiative:** In an effort to increase cybersecurity awareness and education among the States, DHS, through US-CERT and the MS-ISAC, has launched a joint partnership to develop a series of national Web casts that will examine critical and timely cybersecurity issues. The purpose of this initiative is to strengthen the Nation's cyber readiness and resilience.
- **Technical Cybersecurity Alerts:** Written for systems administrators and experienced users, technical alerts provide timely information on current cybersecurity issues and vulnerabilities.

US-CERT also provides a method for citizens, businesses, and other institutions to communicate and coordinate directly with the Federal Government on matters of cybersecurity. The private sector can use the protections afforded by the Protected Critical Infrastructure Information Act to electronically submit proprietary data to US-CERT.

1A.4.2 International Coordination on Cybersecurity

The Federal Government proactively uses its intelligence capabilities to protect the country from cyber attack, its diplomatic outreach and operational capabilities to build partnerships in the global community, and its law enforcement capabilities to combat cyber crime wherever it originates. The private sector, international industry associations, and companies with global interests and operations are also engaged in addressing cybersecurity internationally. For example, the U.S.-based Information Technology Association of America participates in international cybersecurity conferences and forums, such as the India-based National Association for Software and Service Companies Joint Conference. These efforts involve interaction with both the policy and operational communities to coordinate national and international activities that are mutually supportive around the globe:

- **International Cybersecurity Outreach:** DHS, in conjunction with the DOS and other Federal agencies, engages in multilateral and bilateral discussions to further international security awareness and policy development, as well as incident response team information-sharing and capacity-building objectives. The United States engages in bilateral discussions on important cybersecurity issues with close allies and others with whom the United States shares networked interdependencies, to include, but not limited to, Australia, Canada, Egypt, Germany, Hungary, India, Italy, Japan, the Netherlands, Romania, the United Kingdom, etc. The United States also provides leadership in multilateral and regional forums addressing cybersecurity and CIKR protection to encourage all nations to take systematic steps to secure their networked systems. For example, U.S. initiatives include the APEC Telecommunications Working Group capacity-building program to help member countries develop CSIRTs and the OAS framework proposal to create a regional computer incident response point-of-contact network for information sharing and to help member countries develop CSIRTs. Other U.S. efforts to build a culture of cybersecurity include participation in OECD, G8, and United Nations activities. The U.S. private sector is actively involved in this international outreach in partnership with the Federal Government.
- **Collaboration on Cyber Crime:** The U.S. outreach strategy for comprehensive cyber laws and procedures draws on the Council of Europe Convention on Cyber Crime, as well as on the following: (1) the G8 High-Tech Crime Working Group's principles for fighting cyber crime and protecting critical information infrastructure; (2) the OECD guidelines on information and network security; and (3) the United Nations General Assembly resolutions based on the G8 and OECD efforts. The goal of this outreach strategy is to encourage individual nations and regional groupings of nations to join DHS in its efforts to protect internationally interconnected national systems.
- **Collaborative Efforts for Cyber Watch, Warning, and Incident Response:** The Federal Government is working strategically with key allies on cybersecurity policy and operational cooperation. For example, DHS is leveraging pre-existing relationships among CSIRTs. DHS also has established a preliminary framework for cooperation on cybersecurity policy, watch, warning, and incident response with key allies. The framework also incorporates efforts related to key strategic issues as agreed on by these allies. An IWWN is being established among cybersecurity policy, computer emergency response, and law enforcement participants representing 15 countries. The IWWN will provide a mechanism through which the participating countries can share information in order to build global cyber situational awareness and coordinate incident response.
- **Partnerships to Address the Cyber Aspects of Critical Infrastructure Protection:** DHS and the SSAs are leveraging existing agreements, such as the SPP and the JCG with the United Kingdom, to address the IT Sector and cross-cutting cyber components of CIKR protection. The trilateral SPP builds on existing bilateral agreements between the United States and Canada and the United States and Mexico by allowing issues to be addressed on a dual binational basis. In the context of the JCG, DHS established a 10-point action plan to address cybersecurity policy, watch, warning, incident response, and other strategic initiatives.

1A.4.3 Training and Education

The National Strategy to Secure Cyberspace highlights the importance of cyberspace security training and education. Education and training are strategic initiatives in which DHS and other Federal agencies are actively engaged to affect a greater awareness and participation in efforts to promote cybersecurity in the future.

The Federal Government has undertaken several initiatives in partnership with the research and academic communities to better educate and train future cybersecurity practitioners:

- DHS developed the IT Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development. The EBK characterizes the IT security workforce and provides a national baseline representing the essential knowledge and skills that IT security practitioners should have to perform specific roles and responsibilities. Specifically, the EBK does the following:
 - Articulates the functions that professionals within the IT security workforce perform in a context-neutral format and language;
 - Promotes uniform competency guidelines to increase the overall efficiency of IT security education, training, and professional development; and
 - Provides content guidelines that can be leveraged to facilitate cost-effective professional development of the IT workforce, including future skills training and certification, academic curricula, or other affiliated human resources activities.
- DHS co-sponsors the National CAEIAE program with NSA. There are now 94 centers of academic excellence across 38 States. Together, DHS and NSA are working to expand the program to more universities.
- DHS collaborates with the National Science Foundation to co-sponsor and expand the Federal Cyber Services: Scholarship for Service Program. The Scholarship for Service Program provides grant money to selected CAEIAE universities to fund the final 2 years of bachelor's, master's, or doctoral study in information assurance in exchange for an equal amount of time spent working for the Federal Government.
- In fiscal year 2004, the joint DHS/Treasury Computer Investigative Specialist program trained 48 Federal criminal investigators in basic computer forensics. Agents from ICE, the Internal Revenue Service, and the U.S. Secret Service attended the basic 6½-week course. This training was funded through the Treasury Executive Office of Asset Forfeiture.
- Through DHS, DOJ, DoD, and DOS, the Federal Government provides cyber-related training to foreign cyber incident responders (incident response management, creation of CSIRTs) and law enforcement personnel and jurists (law, computer forensics, case handling).

1A.4.4 Research and Development

The Cyber Security Research and Development Act of 2002 authorized a multi-year effort to create more secure cyber technologies, expand cybersecurity R&D, and improve the cybersecurity workforce.

To further address cyber R&D needs, the White House's OSTP established a Cyber Security and Information Assurance Interagency Working Group (CSIA IWG) under the NSTC. The CSIA IWG was jointly chartered by NSTC's Subcommittee on Networking and Information Technology R&D and the Subcommittee on Infrastructure. This interagency working group includes participants from 20 organizations representing 11 departments and agencies, as well as several offices in the White House.

The purpose of the working group is to coordinate Federal programs for cybersecurity and information assurance R&D. It also is responsible for developing the Federal Plan for Cyber Security and Information Assurance R&D, which includes near-term, mid-term, and long-term cybersecurity research efforts in response to the National Strategy to Secure Cyberspace and HSPD-7. The document includes descriptions of approximately 50 cybersecurity R&D topics, such as: Automated Attack Detection, Warning, and Response; Forensics, Traceback, and Attribution; Security Technology and Policy Management Methods; Policy Specification Languages; and Integrated, Enterprise-Wide Security Monitoring and Management. The document also identifies the top cybersecurity and information assurance research topics across the Federal Government. Finally, the document includes key findings and recommendations. DHS actively co-chairs the CSIA IWG with OSTP and continues to identify critical cyber R&D requirements for incorporation into Federal R&D planning efforts.

1A.4.5 Exploring Private Sector Incentives

Awareness and understanding of the need for cybersecurity present a challenge for both government and industry. Although cybersecurity requires significant investments in time and resources, an effective cybersecurity program may reduce the likelihood of a successful cyber attack or reduce the impact if a cyber attack occurs. Network disruptions resulting from cyber attacks

can lead to loss of money, time, products, reputation, sensitive information, or even potential loss of life through cascading effects on critical systems and infrastructure. From an economic perspective, cyber attacks have resulted in billions of dollars of business losses and damages in the aggregate.

The private sector makes risk management decisions, including those for cybersecurity, based on the return on investment and the desire to ensure business continuity. Market-based incentives for cybersecurity investments include protection of intellectual capital, security-influenced procurement, market differentiation, and public confidence. Sometimes, however, cyber assets, systems, or networks may be deemed to be nationally critical and necessitate additional risk management beyond that which the private sector implements as part of their corporate responsibility. To address this difference, the CSCSWG is examining an array of possible incentives for increased investment in cybersecurity.



Appendix 1B: International CIKR Protection

1B.1 Introduction and Purpose of This Appendix

This appendix provides guidance for addressing the international aspects of CIKR protection in support of the NIPP.

1B.1.1 Scope

The NIPP provides the mechanisms, processes, key initiatives, and milestones necessary to enable DHS, DOS, SSAs, and other partners—both foreign and domestic—to strengthen international cooperation to protect U.S. CIKR, both at home and abroad. The NIPP and associated SSPs recognize that protective measures do not stop at a facility’s fence or at a national border. Because disruptions in global infrastructure can have ripple effects around the world, the NIPP and the SSPs also consider cross-border CIKR, international vulnerabilities, and global dependencies and interdependencies.

1B.1.2 Vision

The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets identifies “fostering international cooperation” as one of the eight guiding principles of its vision for the future. The strategy underscores the need for coordinated, comprehensive, and aggressive global action as a key aspect of the NIPP approach to CIKR protection.

This approach involves identifying those CIKR that, if damaged or destroyed, are capable of causing national or regional catastrophic effects on security, public safety, or the economy. HSPD-7 and the 9/11 Commission Act of 2007 support the NIPP mandate to identify the Nation’s critical foreign dependencies so that appropriate risk management strategies may be developed. Furthermore, the National Strategy to Secure Cyberspace sets forth strategic objectives for maintaining national security and ensuring international cooperation on cybersecurity, including preventing cyber attacks against America’s critical infrastructure, reducing vulnerabilities, and building resiliency into systems and networks in order to minimize the damage and recovery time from any cyber attacks and incidents that occur.

1B.1.3 Implementing the Vision With a Strategy for Effective Cooperation

The NIPP strategy for international coordination in CIKR protection outlined in this appendix is focused on effective cooperation with international partners rather than on specific protective measures. Specific measures are tailored to each sector's particular circumstances and are described in the SSPs and addressed as part of the CFI (see section 4.1.4.1). This appendix also discusses existing international agreements that affect CIKR protection and addresses cross-sector and global issues such as the Nation's critical foreign dependencies and cybersecurity.

DHS, DOS, and other concerned Federal departments and agencies work together on an ongoing basis to ensure that the NIPP strategy for international coordination on CIKR protection remains current and is incorporated into the strategies of all Federal partners, as appropriate, to provide a consistent framework for cooperating with other countries and international/multi-national organizations. This effort focuses on: promoting a global culture of physical security and cybersecurity; managing CIKR-related risk beyond the physical borders of the United States; accelerating international cooperation in order to develop intellectual infrastructure based on shared assumptions and compatible conceptual tools; and connecting constituencies not traditionally engaged in CIKR protection. The broad structure of this approach is based on the following high-level considerations.

1B.2 Responsibilities for International Cooperation on CIKR Protection

In accordance with HSPD-7, DOS, in conjunction with DHS, DOJ, DoD, the Departments of Commerce and Treasury, the NRC, and other appropriate departments and agencies, is responsible for working with foreign countries and international/multi-national organizations to strengthen the protection of U.S. CIKR. This section describes the responsibilities of various partners for ensuring and promoting international cooperation in CIKR protection.

1B.2.1 Department of Homeland Security

Under the NIPP risk management framework described in chapter 3, DHS, in collaboration with DOS and other CIKR partners, is responsible for the following actions, all of which have an international dimension:

- Identifying and prioritizing the Nation's critical foreign dependencies through the CFI;
- Building and strengthening international partnerships;
- Implementing a comprehensive, integrated international CIKR risk management program;
- Implementing protective programs and resiliency strategies; and
- Sharing appropriate information with international entities and performing outreach functions to enhance information exchange and management of international agreements on CIKR protection.

Some of the more complex challenges presented by the international aspects of CIKR protection involve analyzing the complex dependencies, interdependencies, and vulnerabilities that require the application of sophisticated and innovative modeling techniques. DHS is responsible for pursuing research and analysis in this area and will call on a range of outside sources for this work, including those with expertise in the international community and the NISAC.

1B.2.2 Department of State

The Secretary of State has direct responsibility for policies and activities related to the protection of U.S. citizens and U.S. facilities abroad and has the overarching lead for U.S. foreign relations, policies, and activities, as well as for the advancement of U.S. interests abroad. The Secretary of State, in conjunction with the Secretary of Homeland Security and specific SSAs, as appropriate, is responsible for coordinating with foreign countries and international organizations to strengthen the protection of critical foreign dependencies. DOS supports the efforts of DHS and other Federal partners by providing knowledge of and access to foreign governments and leveraging bilateral and multilateral relationships around the world to promote the importance of CIKR protection and the priority CIKR, as defined through CFI. In this way, DOS also supports the sharing of best practices related to CIKR protection to ensure that the Federal Government can act effectively to identify and protect U.S. CIKR.

1B.2.3 Other Federal Departments and Agencies

SSAs exchange information, as appropriate, including cyber-specific information, with CIKR partners in other countries. These information-sharing activities are conducted in accordance with guidelines established by DHS and DOS and other Federal departments/agencies to improve the Nation's overall CIKR protection posture.

Under HSPD-7, Federal departments and agencies share the responsibility for working through DOS to reach out to foreign countries and international organizations to strengthen CIKR protection. Federal departments and agencies also have the responsibility for identifying, prioritizing, and managing the risks associated with the Nation's critical foreign dependencies, as well as identifying and prioritizing CIKR located overseas through the CFI.

1B.2.4 State, Local, Tribal, and Territorial Governments

DHS works with State, local, tribal, and territorial governments to help ensure ongoing cooperation with relevant CIKR protection efforts within their jurisdictions and geographic areas. State and local governments, in coordination with DOS and DHS, may also have a cross-border role in regions where there are existing cross-border associations and emergency response agreements.

1B.2.5 Private Sector

DHS works with the private sector and nongovernmental organizations to protect cross-border infrastructure and understand critical foreign dependencies, as well as international and global vulnerabilities. DHS relies on the private sector for data, expertise, and knowledge of their international operations to identify critical international assets, systems, and networks, and assess global risks, including shared threats and interdependencies. DHS uses such information to inform the National Critical Foreign Dependencies List and associated risk management activities.

1B.2.6 Academia

The academic community provides data, insight, and research into the significance of international interdependencies through modeling, simulation, and analysis.

1B.3 Managing the International Dimension of CIKR Risk

The NIPP addresses international CIKR protection, including interdependencies and the vulnerability to threats that originate outside the country. The NIPP brings a new focus to international cooperation and provides a risk-informed strategic framework for measuring the effectiveness of international CIKR protection activities. The NIPP also provides tools to assess international vulnerabilities and interdependencies that complement long-standing cooperative agreements with Canada, Mexico, the United Kingdom, NATO, and others, and supports collaborative engagement with additional international partners.

The SSPs include international considerations as an integral part of each sector's planning process. Some international aspects of CIKR protection require additional overarching or cross-sector emphasis. These include:

- U.S. interactions with foreign governments and international organizations to enhance the confidentiality, integrity, and availability of cyber-based infrastructure, which often has an international or even global dimension;
- Protection of physical assets located on, near, or extending across the borders with Canada and Mexico, or those with important economic supply chain implications that require cooperation with and/or planning and resource allocation among neighboring countries, States bordering these countries, and affected local and tribal governments and the private sector;
- Sectors with CIKR that are extensively integrated into an international or global market (e.g., Banking and Finance or other information-based sectors, Energy, or Transportation Systems), or sectors whose proper functioning relies on input originating from outside the United States; and
- U.S. Government and corporate facilities located overseas (e.g., protection for the Government Facilities Sector involves careful interagency collaboration, as well as cooperation with foreign CIKR partners).

The following subsections discuss issues associated with the international aspects of CIKR protection in the context of the steps of the NIPP risk management framework (see chapter 3).

1B.3.1 Setting Goals and Objectives

The overarching goal of the NIPP—to enhance the protection of U.S. CIKR—applies to the international “system of systems” that underpins U.S. CIKR. The NIPP and the SSPs provide guidance and risk management approaches to address the international aspects of CIKR protection efforts on both a national and a sector-specific level. In addition, a separate set of goals and priorities guides cross-sector and global efforts to improve protection for CIKR with international linkages. These goals fall into three categories:

- Identifying, prioritizing, and addressing cross-sector and global issues;
- Implementing existing and developing new agreements that affect CIKR; and
- Improving the effectiveness of international cooperation.

DHS, in conjunction with DOS and other CIKR partners, defines the requirement for a comprehensive international CIKR protection strategy. The integration of international CIKR protection considerations and measures into each SSP supports the pursuit and achievement of these goals in ways that complement each other and are achievable with the resources available. Important considerations in achieving these goals are discussed in this section.

1B.3.2 Identifying CIKR Affected by International Linkages or Located Internationally

Once international CIKR protection goals and objectives are set, the next step in the risk management process is to develop and maintain a comprehensive inventory of the Nation’s CIKR located outside U.S. borders and of foreign CIKR, the damage or destruction of which may lead to loss of life in the United States or critically affect the Nation’s public health, economy, or national and homeland security capabilities. The process for identifying these CIKR involves working with U.S. industry, SSAs, academia, and international partners to gather and protect information on the foreign infrastructure and resources on which the United States relies or which significantly affect U.S. interests as noted above. This process has been formalized through the CFDI, and results in a prioritized list of assets and systems critical to effectively managing international risks in the CIKR protection mission area.

The NIPP risk management framework details a structured approach for determining dependencies and interdependencies, including physical, cyber, and international considerations. This approach is designed to address CIKR protection needs and vulnerabilities in three areas:

- Direct international linkages to U.S. physical, human, and cyber CIKR:
 - Foreign cross-border assets linked to U.S. CIKR (e.g., roads, bridges, rail lines, pipelines, gas lines, telecommunications lines and undersea cables and facilities, and power lines physically connecting U.S. CIKR to Canada and Mexico);
 - Foreign infrastructure, the disruption or destruction of which could directly harm the U.S. homeland (e.g., a Canadian dam that could flood U.S. territory, a Mexican chemical plant that could affect U.S. territory, or foreign ports and facilities where security failures could directly affect U.S. security); and
 - U.S. CIKR that is located overseas (e.g., non-military government facilities or overseas components of U.S. CIKR).
- Indirect international linkages to physical, human, and cyber U.S. CIKR:
 - The potential cascading and escalating effects of disruptions to foreign assets, systems, and networks such as critical foreign technology, goods and services, resources, transit routes, and chokepoints; and
 - Foreign ownership, control, or involvement in U.S. CIKR and related issues.
- Global aspects of physical and cyber U.S. CIKR:

- Assets, systems, and networks located around the world or with global mobility that require the efforts of multiple foreign countries to effectively manage the associated risks to CIKR.

Analysis of the dependencies and interdependencies is based primarily on information from each sector and the input of CIKR owners and operators regarding their supply chains and sources of services from other infrastructure sectors (e.g., Energy and Water). As the capability for sophisticated network analysis grows, these inputs are complemented by assessments that examine less apparent dependencies and interdependencies. The NISAC supports this effort by analyzing national and international dependencies and interdependencies for complex systems and networks.

1B.3.3 Assessing Risks

Risk assessment for CIKR affected by international linkages is an integral part of the risk management framework described in the NIPP. The risk management framework combines consequences, threats, and vulnerabilities to produce systematic and comprehensive risk assessments that are summarized in the following three-step process that applies equally to CIKR with international linkages:

- Determine the consequences of destruction, incapacitation, or exploitation of CIKR. This is done to assess the potential national significance, as well as physical, cyber, and human dependencies and interdependencies that may result from international linkages.
- Analyze vulnerabilities, including determining which elements of CIKR are most susceptible to attack or disruption (this includes analyzing whether particular international linkages increase the attractiveness of these elements as a target of an attack).
- Conduct a threat analysis to identify the likelihood that a target will be attacked. CIKR with international linkages may present greater opportunities for attack.

Issues important to other countries may differ from those of primary importance to the United States. Risk analysis needs to be conducted in coordination with other countries to draw on their perspectives and expertise, as well as our own.

1B.3.4 Prioritizing CIKR

Assessing CIKR on a level playing field that adjudicates risk based on a common framework ensures that resources are applied where they offer the most benefit for: reducing risk; deterring threats; and minimizing the consequences of attacks, natural disasters, and other emergencies. The HITRAC, through the CFDI and the NISAC, and in coordination with DOS and other public and private sector partners, is responsible for developing the Nation's prioritized list of critical foreign dependencies. Such prioritization helps to inform national goals, foreign engagement, and allows the NIPP community to pursue a coordinated strategy for CIKR risk management. The CFDI is described in greater detail below.

In accordance with the NIPP, the Federal Government created an initial inventory of infrastructure located outside the United States that if disrupted or destroyed would lead to loss of life in the United States or critically affect the Nation's economy or national security. Using this inventory as a starting point, DHS worked with DOS to develop the CFDI, a process designed to ensure that the resulting classified list of critical foreign dependencies is representative and leveraged in a coordinated and inclusive manner.

- **Phase I—Identification (annual):** DHS, working with other Federal partners, developed the first-ever National Critical Foreign Dependencies List in FY2008, reflecting the critical foreign dependencies of the CIKR sectors, as well as critical foreign dependencies of interest to the Nation as a whole. The identification process includes input from public and private sector CIKR community partners.
- **Phase II—Prioritization (annual):** DHS, in collaboration with other CIKR community partners and, in particular, DOS, prioritized the National Critical Foreign Dependencies List based on factors such as the overall criticality of the CIKR to the United States and the willingness and capability of foreign partners to engage in collaborative risk management activities.
- **Phase III—Engagement (ongoing):** Phase III involves leveraging the prioritized list to guide current and future U.S. bilateral and multilateral incident and risk management activities with foreign partners. DHS and DOS established mechanisms to ensure coordinated engagement and collaboration by public entities, in partnership with the private sector.

1B.3.5 Implementing Programs

The SSAs, in collaboration with other CIKR partners, are responsible for developing protective measures to address risks arising from international factors that affect CIKR within their sectors. In addition to sector protective measures, DHS has specific programs to help enhance the cooperation and coordination needed to address the unique challenges posed by international CIKR protection:

- **International Outreach Program:** DHS works with DOS and other Federal departments and agencies with foreign affairs responsibilities to conduct international outreach with foreign countries and international organizations to encourage the promotion and adoption of organizational and policymaking structures, information-sharing mechanisms, industry partnerships, best practices, training, and other programs as needed to improve the protection of overseas assets and the reliability of foreign infrastructure on which the United States depends. These efforts reflect the prioritization of international CIKR and serve as an extension of the CFDI's engagement phase.
- **National Cyber Response Coordination Group (NCRCG):** The NCRCG facilitates coordination of the Federal Government's efforts to prepare for, respond to, and recover from cyber incidents and physical attacks that have significant cyber consequences (collectively known as cyber incidents). It serves as the Federal Government's principal interagency mechanism for operational information sharing and coordination of Federal response and recovery efforts during a cyber incident. The NCRCG consults with international partners for routine situational awareness and during incidents. NCRCG member agencies integrate their capabilities to facilitate assessment of the domestic and international scope and severity of a cyber incident.
- **National Exercise Program (NEP):** DHS provides overarching coordination for the NEP to ensure the Nation's readiness to respond in an all-hazards environment and to test the steady-state protection plans and programs put in place by the NIPP. The NEP provides opportunities through exercises for international partners to engage with Federal, State, and local departments and agencies to address cooperation and cross-border issues, including those related to CIKR protection. DHS and other CIKR partners also participate in exercises sponsored by international partners, including cross-border, multi-sector tabletop exercises.
- **National Cyber Exercises:** DHS conducts exercises to identify, test, and improve the coordination of the cyber incident response community, including Federal, State, local, tribal, territorial, and international governmental entities, as well as private sector corporations and coordinating councils.

Because of the complex nature of the international dimension of CIKR, a substantial emphasis is placed on best practices that can be used to improve cooperation and coordination. To this end, DHS leads efforts to:

- Collaborate to establish best practices and successful protective measures related to telecommunications, air transportation systems, container shipping, cybersecurity, and other global systems, as appropriate;
- Encourage the development of, adoption of, and adherence to the standards of the International Organization for Standards and similar organizations to help reduce insurance premiums and level CIKR protection costs for businesses; and
- Work with international partners to determine the appropriate threshold for engagement with countries on cyber issues.

1B.3.6 Measuring Effectiveness and Making Improvements

Metrics are used to manage the comprehensive international CIKR protection strategy outlined in the NIPP and to track progress toward the strategy's three goals:

- Improving the effectiveness of international cooperation;
- Implementing existing and developing new agreements that affect CIKR; and
- Addressing cross-sector and global CIKR protection issues.

DHS, in cooperation with other Federal departments and agencies, develops data and metrics to track progress on international CIKR protection activities. These data and metrics include:

- The international issues faced by each sector that affect multiple sectors and the relative importance of these issues;
- The countries that should be involved in protection partnerships for each sector;
- The number and type of bilateral and multinational agreements that affect CIKR protection;
- The nature, extent, and effectiveness of bilateral and multinational agreements;
- The sectors affected by each international partnership;
- The number and type of outcomes enabled by an international initiative; and
- Where possible, the specific CIKR protection enhancements that directly result from a particular international initiative.

1B.4 Organizing International CIKR Protection Cooperation

DHS, in conjunction with DOS and other Federal departments and agencies, works with individual foreign governments, as well as regional and international organizations, to enhance CIKR protection on an international basis and to deny opportunities for exploitation of CIKR assets. Potential partnerships depend on:

- Physical proximity to the United States or U.S. CIKR;
- Useful experience and information to be gained from other countries;
- Existing relationships, alliances, agreements, and high-level commitments; and
- Critical supply chains and vulnerable nodes.

As international CIKR protection partnerships mature, cooperative efforts strengthen in two dimensions:

- Development of new partnerships with countries possessing useful experience and information regarding CIKR protection efforts, as well as terrorism prevention, preparedness, response, and recovery; and
- Development of new international relationships and frameworks to protect global infrastructure and address international interdependencies, networked technologies, and the need for a global culture of physical security and cybersecurity.

The coordination mechanisms supporting the NIPP create linkages between CIKR protection efforts at the national, sector, State, local, tribal, territorial, regional, and international levels. A diverse group of entities is involved with this coordination, based on the specific issues that they address, as well as other considerations, as discussed in this section.

1B.4.1 U.S. and Foreign Government Activities and Interactions

DHS works with domestic and international CIKR partners to exchange experiences and information, and to develop a cooperative relationship that will result in material improvement in U.S. CIKR protection, information sharing, cybersecurity, and global telecommunications standards. Through efforts such as the CFDI, DHS, DOS, and other Federal partners work with specific countries to identify international interdependencies and vulnerabilities. The SSAs address international factors such as cross-border infrastructure, international vulnerabilities, and global interdependencies in their SSPs.

The International Affairs offices in Federal departments and agencies maintain relationships with their counterpart foreign ministries and agencies, and play a principal role with DOS in coordinating with foreign governments on international CIKR matters.

International cooperation on issues such as cybersecurity and energy supply is necessary because of the global nature of these types of infrastructure. Such efforts require interaction on both the policy and operational levels and involve a broad range of entities from both government and the private sector. To address cybersecurity, DHS established a framework for cooperation on cybersecurity policy, watch and warning, and incident response for CIKR with key allies such as Australia, Canada, New Zealand, and the United Kingdom. DHS is coordinating and participating in the establishment of an IWWN among policy,

computer emergency response, and law enforcement participants in 15 countries. The IWWN provides an information-sharing mechanism through which participating countries can build cyber situational awareness and coordinate incident response.

DHS, SSAs, and other U.S. partners work with other countries to promote CIKR protection best practices and pursue infrastructure security through international/multilateral organizations such as the Group of Eight (G8), NATO, European Union, OAS, OSCE, OECD, and Asia-Pacific Economic Cooperation (APEC). International cooperation on CIKR protection takes place bilaterally, regionally, and multilaterally. The approach to working with some specific countries and organizations is founded on formal agreements that address cooperation on CIKR protection, as described below.

- **Canada and Mexico:** The CIKR of the United States and its immediate neighbors are closely interconnected and cover a wide range of sectors. Electricity, natural gas, oil, telecommunications, roads, rail, food, water, minerals, and finished products cross the borders on a regular basis as part of normal commerce. The importance of this trade, and the infrastructure that supports it, was highlighted after the terrorist attacks of September 11, 2001, nearly closed both borders. The United States entered into the 2001 Smart Border Accord with Canada and the 2002 Border Partnership Plan with Mexico, in part, to address bilateral CIKR issues. In addition, the 2005 SPP established a trilateral approach to common security issues. The SPP complements existing agreements.
- **United Kingdom:** The United Kingdom is a close ally of the United States who has much experience in fighting terrorism and protecting its CIKR. The United Kingdom has developed substantial expertise in law enforcement and intelligence systems, and in the protection of commercial facilities based on its counterterrorism experience. Like the United States, most of the critical infrastructure in the United Kingdom is privately owned. The government of the United Kingdom developed an effective, sophisticated system to manage public-private partnerships. DHS formed a JCG with the United Kingdom that brings officials into regular, formal contact to discuss and resolve a range of bilateral homeland security issues.
- **The Group of Eight (G8):** Since September 11, 2001, the infrastructure in several G8 countries has been exploited and used to inflict casualties and fear. As a result, G8 partners underscored their determination to combat all forms of terrorism and to strengthen international cooperation. To that end, within the G8 context, the United States spearheaded various critical infrastructure protection initiatives in 2007 and 2008. The first project focused on G8 delegation nation security planning best practices, vulnerability assessment methodologies, and threat assessments for critical energy infrastructure. The second project focused on chemical sector infrastructure protection activities, which was a timely subject given the release of the CFATS in the United States during the previous year. These projects have increased the baseline understanding of the measures underway, as well as the CIKR protection capabilities of each G8 member nation. The G8 offers an effective forum through which members can work to reduce global risks to CIKR by sharing best practices and methodologies, and understanding common threats. Future projects related to critical infrastructure protection within the G8 will address issues related to interdependencies within and across infrastructure systems.
- **European Union:** The United States is engaged in a number of CIKR protection and resiliency activities with the European Union, including those related to advising the European Union on CIKR risk analysis and management, writ large, as well as counter-explosive device activities. The European Commission is in the process of implementing the EPCIP. This program will affect all 27 nations in the European Union, as well as potentially others in the Euro-Zone that elect to participate. EPCIP will initially focus on the energy and transport sectors, with expanded focus on the telecommunications, financial, and chemical sectors in coming years. The United States has engaged the EPCIP leadership for the purpose of offering the assistance necessary to support the implementation of the program, with the ultimate goal of enhancing CIKR protection activities wherever they may be found. Furthermore, IP and S&T work with the DOS Bureau of Diplomatic Security's Office of Anti-terrorism Assistance and the Office of the Coordinator for Counterterrorism, DOJ, and FBI to coordinate with the European Union to conduct workshops, seminars, and exercises on countering terrorist use of explosive devices.
- **North Atlantic Treaty Organization (NATO):** NATO addresses CIKR issues through the Senior Civil Emergency Planning Committee, the senior policy and advisory body to the North Atlantic Council on civil emergency planning and disaster relief matters. The committee is responsible for policy direction and coordination of Planning Boards and Committees in the NATO environment. It has developed considerable expertise that applies to CIKR protection and has implemented planning boards and committees covering ocean shipping, inland surface transport, civil aviation, food and agriculture, industrial prepared-

ness, civil communications planning, civil protection, and civil-military medical issues. DHS: provides a delegation to the Senior Civil Emergency Planning Committee at NATO; participates in NATO's telecommunications working group and the critical infrastructure protection coordination group; has expert NATO representation on the Civil Protection Committee and Industrial Planning Committee; and engages with NATO in preparedness exercises.

1B.4.2 Foreign Investment in U.S. CIKR

CIKR protection may be affected by foreign investment and ownership of sector assets. At the Federal level, this issue is monitored by the CFIUS. The committee is chaired by the Secretary of the Treasury, with membership that includes: the Secretaries of State, Defense, Commerce, and Homeland Security; the Attorney General; the Directors of the OMB and the OSTP; the U.S. Trade Representative; the Chairman of the Council of Economic Advisors; the Assistant to the President for Economic Policy; and the Assistant to the President for National Security Affairs. The CFIUS is the Federal inter-agency body charged with addressing potential conflicts between maintaining open U.S. markets and ensuring national and homeland security.

As a member of CFIUS, DHS examines the potential impact of proposed foreign investments on current and planned CIKR protection activities. The committee develops and negotiates security agreements with foreign entities to manage any CIKR risks that foreign investment may pose. DHS leads government monitoring activities to ensure compliance with these agreements.

DHS also partners with DOJ and other Federal departments and agencies to review applications to the FCC from foreign entities pursuant to section 214 of the Communications Act of 1934. DHS supports these reviews to assess whether the proposed activities pose any threat to CIKR protection.

1B.4.3 Information Sharing

Effective international cooperation on CIKR protection requires information-sharing systems that include processes and protocols for real-time information sharing and communication of threats and relevant intelligence reports. Successful international cooperation also requires mechanisms for the systematic sharing of best practices and frequent opportunities for partners to meet in order to discuss international CIKR issues.

The NOC serves as the Nation's hub for information sharing and situational awareness for domestic incident management and is responsible for increasing coordination (through the NICC) among those members of the international community who are involved because of the role that they play in enabling the protection of U.S. CIKR.

The HSIN supports ongoing information-sharing efforts by offering COIs for selected international partners requiring close coordination with the NICC and NOC.

DHS also provides mechanisms (e.g., the US-CERT portal) to improve information sharing and coordination among government communities and selected international partners for cybersecurity. The Cybercop portal is a secure, Internet-based information-sharing mechanism for law enforcement personnel involved in electronic crimes investigation. This collaborative tool links the law enforcement community worldwide, supporting participants from more than 40 countries.

1B.5 Ensuring International Cooperation Over the Long Term

Ensuring a sustainable approach to the international aspects of CIKR protection over the long term requires special consideration in the following areas:

- **Awareness:** Awareness of international aspects of CIKR protection issues helps ensure implementation of effective, coordinated, and integrated CIKR protection measures and enables CIKR partners to make informed decisions. Often, these issues are not apparent to those who can take the most effective action because of the complexity of the international systems affecting CIKR protection. Awareness programs designed to identify and address such issues are required to ensure continued international support for protection programs over the long term. DHS is collaborating with DOS and other NIPP partners to build awareness of the international aspects of CIKR protection and their importance in developing effective protective programs and resiliency strategies in this global age.

- **Training and Education:** NIPP training courses for the managers and staff responsible for CIKR should cover international considerations for CIKR protection because of the complex issues that often accompany international linkages and initiatives. DHS ensures that the organizational and sector expertise needed to implement the international aspects of the NIPP program over the long term are developed and maintained through exercises and other mechanisms that promote international cooperation on CIKR protection. For example, IP, S&T, DOS, and DOJ work with the European Union to conduct workshops, seminars, and exercises on methods and technologies for countering explosive devices.
- **Research and Development:** Cooperative and coordinated R&D efforts are one of the most effective ways to improve protective capabilities or dramatically lower the costs of existing capabilities so that international CIKR partners can afford to do more with limited resources. Techniques and designs developed through research can cost very little to share with international CIKR partners and, although the lead times needed for maturation of technology from the laboratory to the field can be decades, such improvements can have wider applicability or much greater effectiveness than available through current methods. Several Federal departments and agencies monitor international R&D efforts to avoid duplication and identify projects that may affect U.S. Government interests and activities. For example, S&T's International Programs Division evaluates international R&D projects that S&T may leverage to benefit U.S. homeland security and CIKR protection efforts. DHS, DoD, DOE, and DOJ all collaborate with international partners, as does the interagency TSWG, to develop technological solutions to defeat terrorism threats, including threats to CIKR.
- **Vulnerability Assessments:** Over the past several years, DHS has worked with U.S. interagency partners in DOS, DOE, and the U.S. Army Corps of Engineers, among others, to conduct vulnerability assessments on international CIKR of interest to the United States. These assessments have included essential bridges and tunnels at the northern border with Canada, critical dams at the southern border with Mexico, locks and levees in Panama, and Energy Sector installations in a Caribbean nation. The purpose of these assessments is to protect U.S. interests abroad and to provide assistance, training, and other support to U.S. allies and partners. As the critical infrastructure protection capabilities within the United States continue to mature, more nations will seek assistance and expertise from the United States and the United States will continue to identify CIKR assets of interest on foreign or shared soil. Opportunities to increase the global CIKR protection posture should be undertaken where appropriate.
- **Plan Updates:** Annual reviews and updates of the NIPP and SSPs must consider the current international situation and be coordinated, as appropriate, with international agreements affecting CIKR protection. As the SSPs are reviewed for reissue in 2010, they will reflect, as appropriate, updated information on the CFDI, the status of relevant international agreements, and other international CIKR protection efforts.

Appendix 2: Summary of Relevant Statutes, Strategies, and Directives

This summary provides additional information on a variety of statutes, strategies, and directives referenced in chapters 2 and 5, as applicable to CIKR protection. This list is not inclusive of all authorities related to CIKR protection; rather, it includes the authorities most relevant to national-level, cross-sector CIKR protection. Please note that there are many other authorities that are related to specific sectors that are not discussed in this appendix; these are left for further elaboration in the SSPs.

2.1 Statutes

Homeland Security Act of 2002⁹

This act establishes a Cabinet-level department headed by a Secretary of Homeland Security with the mandate and legal authority to protect the American people from the continuing threat of terrorism. In the act, Congress assigns DHS the primary missions to:

- Prevent terrorist attacks within the United States;
- Reduce the vulnerability of the United States to terrorism at home;
- Minimize the damage and assist in the recovery from terrorist attacks that occur; and
- Ensure that the overall economic security of the United States is not diminished by efforts, activities, and programs aimed at securing the homeland.

This statutory authority defines the protection of CIKR as one of the primary missions of the department. Among other actions, the act specifically requires DHS:

- To carry out comprehensive assessments of the vulnerabilities of U.S. CIKR, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks;
- To develop a comprehensive national plan for securing the CIKR of the United States, including power production, generation, and distribution systems; IT and telecommunications systems (including satellites); electronic financial and property record storage and transmission systems; emergency preparedness communications systems; and the physical and technological assets that support such systems; and

⁹ Public Law 107-296, November 25, 2002, 116 Stat. 2135. It is coded at 6 U.S.C.

- To recommend measures necessary to protect U.S. CIKR in coordination with other agencies of the Federal Government and in cooperation with State and local government agencies and authorities, the private sector, and other entities.

Those requirements, combined with the President's direction in HSPD-7, mandate the unified approach to CIKR protection taken in the NIPP.

Critical Infrastructure Information Act of 2002¹⁰

Enacted as part of the Homeland Security Act, this act creates a framework that enables members of the private sector and others to voluntarily submit sensitive information regarding the Nation's CIKR to DHS with the assurance that the information, if it satisfies certain requirements, will be protected from public disclosure.

The PCII Program, created under the authority of the act, is central to the information-sharing and protection strategy of the NIPP. By protecting sensitive information submitted through the program, the private sector is assured that the information will remain secure and only be used to further CIKR protection efforts.¹¹

Implementing Recommendations of the 9/11 Commission Act of 2007

This act requires the implementation of some of the recommendations made by the 9/11 Commission, to include requiring the Secretary of Homeland Security to: (1) establish department-wide procedures to receive and analyze intelligence from State, local, and tribal governments and the private sector; and (2) establish a system that screens 100 percent of maritime and passenger cargo.

Section 1002 of the act includes a requirement for DHS to report annually to Congress on the comprehensive risk assessments carried out for each CIKR sector, to include an evaluation of threats, vulnerabilities, and consequences. These reports should describe any actions or countermeasures recommended or taken by DHS or another SSA to address the issues identified in the assessments. This reporting requirement is covered by the National CIKR Protection Annual Report submitted to Congress in November of each year, as well as the Congressional Mid-Year Brief delivered to Congress each Spring.

This act establishes the International Border Community Interoperable Communications Demonstration Project, which helps identify and implement solutions to cross-border communications and cooperation, and the Interagency Threat Assessment and Coordination Group (ITACG), which improves interagency communications. The establishment of ITACG Advisory Councils allows Federal agencies to set policies to improve communication within the information-sharing environment and supports establishment of an ITACG Detail that gives State, local, and tribal homeland security officials, law enforcement officers, and intelligence analysts the opportunity to work in the National Counterterrorism Center.

The act also established grants to support high-risk urban areas and State, local, and tribal governments in preventing, preparing for, protecting against, and responding to acts of terrorism, and to assist States in carrying out initiatives to improve international emergency communications.

Title IX of the act requires DHS to establish a common set of criteria for private sector preparedness in disaster management, emergency management, and business continuity. These Voluntary Private Sector Preparedness Standards will be accredited and certified by ANSI and the ASQ ANAB. An internal DHS Private Sector Preparedness Council will be responsible for: selecting program standards; defining and promoting the business case for private sector entities to work toward voluntary certification; overseeing the program's progress; and providing regular updates to Congress.

Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act)¹²

The Stafford Act provides comprehensive authority for response to emergencies and major disasters—natural disasters, accidents, and intentionally perpetrated events. It provides specific authority for the Federal Government to provide assistance to State and local entities for disaster preparedness and mitigation, and major disaster and emergency assistance. Major disaster and emergency assistance includes such resources and services as:

¹⁰ The CII Act is presented as subtitle B of title II of the Homeland Security Act (sections 211-215) and is codified at 6 U.S.C. 131 et seq.

¹¹ Procedures for Handling Critical Infrastructure Information, 68 Fed. Reg. 8079 (Feb. 20, 2004), are codified at 6 CFR Part 29.

¹² Public Law 93-288, as amended, codified at 42 U.S.C. 68.

- The provision of Federal resources, in general;
- Medicine, food, and other consumables;
- Work and services to save lives and restore property, including:
 - Debris removal;
 - Search and rescue; emergency medical care; emergency mass care; emergency shelter; and provision of food, water, medicine, and other essential needs, including movement of supplies or persons;
 - Clearance of roads and construction of temporary bridges;
 - Provision of temporary facilities for schools and other essential community services;
 - Demolition of unsafe structures that endanger the public;
 - Warning of further risks and hazards;
 - Dissemination of public information and assistance regarding health and safety measures;
 - Provision of technical advice to State and local governments on disaster management and control; and
 - Reduction of immediate threats to life, property, and public health and safety;
- Hazard mitigation;
- Repair, replacement, and restoration of certain damaged facilities; and
- Emergency communications, emergency transportation, and fire management assistance.

Disaster Mitigation Act of 2000

This act amends the Stafford Act by repealing the previous mitigation planning provisions (section 409) and replacing them with a new set of requirements (section 322). This new section emphasizes the need for State, local, and tribal entities to closely coordinate mitigation planning and implementation efforts.

Section 322 continues the requirement for a State mitigation plan as a condition of disaster assistance, adding incentives for increased coordination and integration of mitigation activities at the State level through the establishment of requirements for two different levels of State plans—standard and enhanced. States that demonstrate an increased commitment to comprehensive mitigation planning and implementation through the development of an approved Enhanced State Plan can increase the amount of funding available through the Hazard Mitigation Grant Program (HMGP). Section 322 also establishes a new requirement for local mitigation plans and authorizes up to 7 percent of HMGP funds available to a State to be used for development of State, local, and tribal mitigation plans.

Corporate and Criminal Fraud Accountability Act of 2002 (also known as the Sarbanes-Oxley Act)¹³

The act applies to entities required to file periodic reports with the Securities and Exchange Commission under the provisions of the Securities and Exchange Act of 1934, as amended. It contains significant changes to the responsibilities of directors and officers, as well as the reporting and corporate governance obligations of affected companies. Among other items, the act requires certification by the company’s chief executive officer (CEO) and chief financial officer that accompanies each periodic report filed that the report fully complies with the requirements of the securities laws and that the information in the report fairly presents, in all material respects, the financial condition and results of the operations of the company. It also requires certifications regarding internal controls and material misstatements or omissions, and the disclosure on a “rapid and current basis” of information regarding material changes in the financial condition or operations of a public company. The act contains a number of additional provisions dealing with insider accountability and disclosure obligations, and auditor independence. It also provides severe criminal and civil penalties for violations of the act’s provisions.

¹³ Public Law 107-204, July 30, 2002.

The Defense Production Act of 1950 and the Defense Production Reauthorization Act of 2003

This act provides the primary authority to ensure the timely availability of resources for national defense and civil emergency preparedness and response. Among other powers, this act authorizes the President to require that companies accept and give priority to contracts that the President “deems necessary or appropriate to promote the national defense,” and allocate materials, services, and facilities, as necessary, to promote the national defense. This act also authorizes loan guarantees, direct loans, direct purchases, and purchase guarantees for those goods necessary for national defense. It also provides for the review of foreign acquisitions of U.S. businesses in order to identify and resolve any national security risks. This act defines “national defense” to include critical infrastructure protection and restoration, as well as activities authorized by the emergency preparedness sections of the Stafford Act. Consequently, the authority stemming from the Defense Production Act is available for activities and measures undertaken in preparation for, during, or following a natural disaster or accidental or malicious event. Under the act and related Presidential orders, the Secretary of Homeland Security has the authority to place and, upon application, authorize State and local governments to place priority-rated contracts for industrial resources in support of Federal, State, and local emergency preparedness activities. The Defense Production Act has a national security nexus with the NIPP.

The Freedom of Information Act¹⁴

This act generally provides that any person has a right, enforceable in court, to obtain access to Federal agency records, except to the extent that such records are protected from public disclosure by the nine listed exemptions or the three law enforcement exclusions. Persons who make requests are not required to identify themselves or explain the purpose of the request. The underlying principle of FOIA is that the workings of government are for and by the people and that the benefits of government information should be made broadly available. All Federal Government agencies must adhere to the provisions of FOIA with certain exceptions for work in progress, enforcement confidential information, classified documents, and national security information. FOIA was amended by the Electronic Freedom of Information Act Amendment of 1996 and the OPEN Government Act of 2007.

Information Technology Management Reform Act of 1996¹⁵

Under section 5131 of the Information Technology Management Reform Act of 1996, NIST develops standards, guidelines, and associated methods and techniques for Federal computer systems. Federal Information Processing Standards are developed by NIST only when there are no existing voluntary standards to address the Federal requirements for the interoperability of different systems, the portability of data and software, and computer security.

Gramm-Leach-Bliley Act of 1999¹⁶

Among other items, this act (title V) provides limited privacy protections on the disclosure by a financial institution of nonpublic personal information. The act also codifies protections against the practice of obtaining personal information through false pretenses.

Public Health Security and Bioterrorism Preparedness and Response Act of 2002¹⁷

This act improves the ability of the United States to prevent, prepare for, and respond to bioterrorism and other public health emergencies. Key provisions of the act, 42 U.S.C. 247d and 300hh among others, address: (1) development of a national preparedness plan by HHS that is designed to provide effective assistance to State and local governments in the event of bioterrorism or other public health emergencies; (2) operation of the National Disaster Medical System to mobilize and address public health emergencies; (3) grant programs for the education and training of public health professionals and the improvement of State, local, and hospital preparedness for and response to bioterrorism and other public health emergencies; (4) streamlining and clarification of communicable disease quarantine provisions; (5) enhancement of controls on dangerous biological agents and toxins; and (6) protection of the safety and security of food and drug supplies.

¹⁴ Codified as 5 U.S.C. 552.

¹⁵ Public Law 104-106.

¹⁶ Public Law 106-102 (1999), codified at 15 U.S.C. 94.

¹⁷ Public Law 107-188.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)¹⁸

This act outlines the domestic policy related to deterring and punishing terrorists, and the U.S. policy for CIKR protection. It also provides for the establishment of a national competence for CIKR protection. The act establishes the NISAC and outlines the Federal Government's commitment to understanding and protecting the interdependencies among critical infrastructure.

The Privacy Act of 1974¹⁹

This act provides strict limits on the maintenance and disclosure by any Federal agency of information on individuals that is maintained, including "education, financial transactions, medical history, and criminal or employment history and that contains [the] name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." Although there are specific categories for permissible maintenance of records and limited exceptions to the prohibition on disclosure for legitimate law enforcement and other specified purposes, the act requires strict recordkeeping on any disclosure. The act also specifically provides for access by individuals to their own records and for requesting corrections thereto.

Federal Information Security Management Act of 2002²⁰

This act requires that Federal agencies develop a comprehensive information technology security program to ensure the effectiveness of information security controls over information resources that support Federal operations and assets. This legislation is relevant to the part of the NIPP that governs the protection of Federal assets and the implementation of cyber-protective measures under the Government Facilities SSP.

Cyber Security Research and Development Act of 2002²¹

This act allocates funding to NIST and the National Science Foundation for the purpose of facilitating increased R&D for computer network security and supporting research fellowships and training. The act establishes a means of enhancing basic R&D related to improving the cybersecurity of CIKR.

Maritime Transportation Security Act of 2002²²

This act directs initial and continuing assessments of maritime facilities and vessels that may be involved in a transportation security incident. It requires DHS to prepare a National Maritime Transportation Security Plan for deterring and responding to a transportation security incident and to prepare incident response plans for facilities and vessels that will ensure effective coordination with Federal, State, and local authorities. It also requires, among other actions, the establishment of: transportation security and crewmember identification cards and processes; maritime safety and security teams; port security grants; and enhancements to maritime intelligence and matters dealing with foreign ports and international cooperation.

Atomic Energy Act of 1954

The Atomic Energy Act of 1954, as amended in NUREG-0980, provides for both the development and regulation of civilian uses of nuclear materials and facilities in the United States. The act requires that civilian uses of nuclear materials and facilities be licensed and it empowers the NRC to establish, by rule or order, standards to govern these uses.

Intelligence Reform and Terrorism Prevention Act of 2004²³

This act provides sweeping changes to the U.S. Intelligence Community structure and processes, and creates new systems that are specially designed to combat terrorism. Among other actions, the act:

¹⁸ Public Law 107-56, October 26, 2001.

¹⁹ Codified at 5 U.S.C. 552a.

²⁰ Public Law 107-347, December 17, 2002.

²¹ Public Law 107-305, November 27, 2002.

²² Public Law 107-295, codified at 46 U.S.C. 701.

²³ Public Law 108-458.

- Establishes a Director of National Intelligence with specific budget, oversight, and programmatic authority over the Intelligence Community;
- Establishes the National Intelligence Council and redefines “national intelligence”;
- Requires the establishment of a secure ISE and an information-sharing council;
- Establishes a National Counterterrorism Center, a National Counterproliferation Center, National Intelligence Centers, and a Joint Intelligence Community Council;
- Establishes, within the EOP, a Privacy and Civil Liberties Oversight Board;
- Requires the Director of the FBI to continue efforts to improve the intelligence capabilities of the FBI and to develop and maintain, within the FBI, a national intelligence workforce;
- Directs improvements in security clearances and clearance processes;
- Requires DHS to: develop and implement a National Strategy for Transportation Security and transportation modal security plans; enhance identification and credentialing of transportation workers and law enforcement officers; conduct R&D into mass identification technology, including biometrics; enhance passenger screening and terrorist watch lists; improve measures for detecting weapons and explosives; improve security related to the air transportation of cargo; and implement other aviation security measures;
- Directs enhancements to maritime security;
- Directs enhancements in border security and immigration matters;
- Enhances law enforcement authority and capabilities, and expands certain diplomatic, foreign aid, and military authority and capabilities for combating terrorism;
- Requires expanded machine-readable visas with biometric data; implementation of a biometric entry and exit system, and a registered traveler program; and implementation of biometric or other secure passports;
- Requires standards for birth certificates and driver’s licenses or personal identification cards issued by States for use by Federal agencies for identification purposes and enhanced regulations for social security cards;
- Requires DHS to improve preparedness nationally, especially measures to enhance interoperable communications and to report on vulnerability and risk assessments of the Nation’s CIKR; and
- Directs measures to improve assistance to and coordination with State, local, and private sector entities.

2.2 National Strategies and Implementation Plans

The National Strategy for Homeland Security (July 2002)

This strategy establishes the Nation’s strategic homeland security objectives and outlines the six critical mission areas necessary to achieve those objectives. The strategy also provides a framework to align the resources of the Federal budget directly to the task of securing the homeland. The strategy specifies eight major initiatives to protect the Nation’s CIKR, one of which specifically calls for the development of the NIPP.

National Strategy for Homeland Security (October 2007)

The updated strategy serves to guide, organize, and unify our Nation’s homeland security efforts. It is a national strategy (not a Federal strategy) that articulates the approach to secure the homeland over the next several years. It builds on the first National Strategy for Homeland Security, issued in July 2002, and complements both the National Security Strategy issued in March 2006 and the National Strategy for Combating Terrorism, issued in September 2006. It reflects the increased understanding of threats confronting the United States, incorporates lessons learned from exercises and real-world catastrophes, and addresses ways to ensure long-term success by strengthening the homeland security foundation that has been built.

National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (February 2003)

This strategy identifies the policy, goals, objectives, and principles for actions needed to “secure the infrastructures and assets vital to national security, governance, public health and safety, economy, and public confidence.” The strategy provides a unifying organizational structure for CIKR protection and identifies specific initiatives related to the NIPP to drive near-term national protection priorities and inform the resource allocation process.

National Strategy to Secure Cyberspace (February 2003)

This strategy sets forth objectives and specific actions to prevent cyber attacks against America’s CIKR, reduce nationally identified vulnerabilities to cyber attacks, and minimize damage and recovery time from cyber attacks. The strategy provides the vision for cybersecurity and serves as the foundation for the cybersecurity component of CIKR.

The National Strategy for Maritime Security (September 2005)

This strategy provides the framework to integrate and synchronize the existing department-level strategies and ensure their effective and efficient implementation, and integrates all Federal Government maritime security programs and initiatives into a comprehensive and cohesive national effort involving appropriate Federal, State, local, and private sector entities.

The National Strategy to Combat Weapons of Mass Destruction (December 2002)

This strategy provides policy guidance on combating WMD through three pillars:

- Counterproliferation to combat WMD use;
- Strengthened nonproliferation to combat WMD proliferation; and
- Consequence management to respond to WMD use.

The National Strategy for Combating Terrorism (September 2006)

This strategy provides a comprehensive overview of the terrorist threat and sets specific goals and objectives to combat this threat, including measures to:

- Defeat terrorists and their organizations;
- Deny sponsorship, support, and sanctuary to terrorists;
- Diminish the underlying conditions that terrorists seek to exploit; and
- Defend U.S. citizens and interests at home and abroad.

The National Intelligence Strategy of the United States of America (October 2005)

The National Intelligence Strategy of the United States of America outlines the fundamental values, priorities, and orientation of the Intelligence Community. As directed by the Director of National Intelligence, the strategy outlines the specific mission objectives that relate to efforts to predict, penetrate, and pre-empt threats to national security. To accomplish this, the efforts of the different enterprises of the Intelligence Community are integrated through policy, doctrine, and technology, and by ensuring that intelligence efforts are appropriately coordinated with the Nation’s homeland security mission.

The National Continuity Policy Implementation Plan (August 2007)

The National Continuity Policy Implementation Plan (NCPIP) identifies how the National Continuity Policy described in NSPD-51/HSPD-20 will be translated into action. The NCPIP is a comprehensive and integrated list of directives for the Federal Executive Branch to ensure the effectiveness and survivability of our national continuity capability. It is also an educational primer for State, local, tribal, and territorial governments and private sector partners that support the Nation’s continuity capability.

2.3 Homeland Security Presidential Directives

HSPD-1: Organization and Operation of the Homeland Security Council (October 2001)

HSPD-1 establishes the Homeland Security Council and a committee structure for developing, coordinating, and vetting homeland security policy among executive departments and agencies. The directive provides a mandate for the Homeland Security Council to ensure the coordination of all homeland security-related activities among executive departments and agencies, and promotes the effective development and implementation of all homeland security policies. The Homeland Security Council is responsible for arbitrating and coordinating any policy issues that may arise among the different departments and agencies covered by the NIPP.

HSPD-2: Combating Terrorism Through Immigration Policies (October 2001)

HSPD-2 establishes policies and programs to enhance the Federal Government's capabilities for preventing aliens who engage in or support terrorist activities from entering the country and for detaining, prosecuting, or deporting any such aliens who are in the United States.

HSPD-2 also directs the Attorney General to create the Foreign Terrorist Tracking Task Force to ensure that, to the maximum extent permitted by law, Federal agencies coordinate programs to accomplish the following: (1) deny entry into the United States of aliens associated with, suspected of being engaged in, or supporting terrorist activity; and (2) locate, detain, prosecute, or deport any such aliens already present in the United States.

HSPD-3: Homeland Security Advisory System (March 2002)

HSPD-3 mandates the creation of an alert system for disseminating information regarding the risk of terrorist acts to Federal, State, and local authorities, and the public. It also includes the requirement for a corresponding set of protective measures for Federal, State, and local governments to be implemented, depending on the threat condition. Such a system provides warnings in the form of a set of graduated threat conditions that are elevated as the risk of the threat increases. For each threat condition, Federal departments and agencies are required to implement a corresponding set of protective measures.

HSPD-4: National Strategy to Combat Weapons of Mass Destruction (December 2002)

This directive outlines a strategy that includes three principal pillars: (1) Counterproliferation to Combat WMD Use, (2) Strengthened Nonproliferation to Combat WMD Proliferation, and (3) Consequence Management to Respond to WMD Use. It also outlines four cross-cutting functions to be pursued on a priority basis: (1) intelligence collection and analysis on WMD, delivery systems, and related technologies; (2) R&D to improve our ability to address evolving threats; (3) bilateral and multilateral cooperation; and (4) targeted strategies against hostile nations and terrorists.

HSPD-5: Management of Domestic Incidents (February 2003)

HSPD-5 establishes a national approach to domestic incident management that ensures effective coordination among all levels of government and between the government and the private sector. Central to this approach is the NIMS, an organizational framework for all levels of government, and the NRF, an operational framework for national incident response.

In this directive, the President designates the Secretary of Homeland Security as the principal Federal official for domestic incident management and empowers the Secretary to coordinate Federal resources used for prevention, preparedness, response, and recovery related to terrorist attacks, major disasters, or other emergencies. The directive assigns specific responsibilities to the Attorney General, Secretary of Defense, Secretary of State, and the Assistants to the President for Homeland Security and National Security Affairs, and directs the heads of all Federal departments and agencies to provide their "full and prompt cooperation, resources, and support," as appropriate and consistent with their own responsibilities for protecting national security, to the Secretary of Homeland Security, Attorney General, Secretary of Defense, and Secretary of State in the exercise of leadership responsibilities and missions assigned in HSPD-5.

HSPD-6: Integration and Use of Screening Information (September 2003)

HSPD-6 consolidates the Federal Government's approach to terrorist screening by establishing a Terrorist Screening Center. Federal departments and agencies are directed to provide terrorist information to the Terrorist Threat Integration Center, which

is then required to provide all relevant information and intelligence to the Terrorist Screening Center. In order to protect against terrorism, this directive established the national policy to: (1) develop, integrate, and maintain thorough, accurate, and current information about individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism (Terrorist Information); and (2) use that information, as appropriate and to the full extent permitted by law, to support: (a) Federal, State, local, tribal, territorial, foreign government, and private sector screening processes; and (b) diplomatic, military, intelligence, law enforcement, immigration, visa, and protective processes.

HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection (December 2003)

HSPD-7 establishes a framework for Federal departments and agencies to identify, prioritize, and protect CIKR from terrorist attacks, with an emphasis on protecting against catastrophic health effects and mass casualties. HSPD-7 mandates the creation and implementation of the NIPP and sets forth the roles and responsibilities for: DHS; SSAs; other Federal departments and agencies; and State, local, tribal, territorial, private sector, and other CIKR partners.

HSPD-8: National Preparedness (December 2003)

HSPD-8 establishes policies to strengthen the preparedness of the United States to prevent, protect, respond to, and recover from threatened or actual domestic terrorist attacks, major disasters, and other emergencies by: requiring a national domestic all-hazards preparedness goal; establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments; and outlining actions to strengthen the preparedness capabilities of Federal, State, and local entities. This directive mandates the development of the goal to guide emergency preparedness training, planning, equipment, and exercises, and to ensure that all entities involved adhere to the same standards. The directive calls for an inventory of Federal response capabilities and refines the process by which preparedness grants are administered, disbursed, and utilized at the State and local levels.

HSPD-9: Defense of U.S. Agriculture and Food (January 2004)

HSPD-9 establishes an integrated national policy for improving intelligence operations, emergency response capabilities, information-sharing mechanisms, mitigation strategies, and sector vulnerability assessments to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies.

HSPD-10: Biodefense for the 21st Century (April 2004)

HSPD-10 outlines the essential pillars of our national biodefense program as: (1) threat awareness; (2) prevention and protection; (3) surveillance and detection; and (4) response and recovery. This directive describes these various disciplines in detail and sets forth objectives for further progress under the national biodefense program, highlighting key roles for Federal departments and agencies. The Secretary of Homeland Security is responsible for coordinating domestic Federal operations to prepare for, respond to, and recover from biological weapons attacks.

HSPD-11: Comprehensive Terrorist-Related Screening Procedures (August 2004)

HSPD-11 requires the creation of a strategy and implementation plan for a coordinated and comprehensive approach to terrorist screening to improve and expand procedures to screen people, cargo, conveyances, and other entities and objects that pose a threat.

HSPD-12: Policy for a Common Identification Standard for Federal Employees and Contractors (August 2004)

HSPD-12 establishes a mandatory, government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors to enhance security, increase governmental efficiency, reduce identity fraud, and protect personal privacy. The resulting mandatory standard was issued by NIST as the Federal Information Processing Standard Publication.

HSPD-13: Maritime Security Policy (December 2004)

HSPD-13 directs the coordination of U.S. Government maritime security programs and initiatives to achieve a comprehensive and cohesive national effort involving the appropriate Federal, State, local, and private sector entities. The directive also establishes a Maritime Security Policy Coordinating Committee to coordinate interagency maritime security policy efforts.

HSPD-14: Domestic Nuclear Detection (April 2005)

HSPD-14 establishes the effective integration of nuclear and radiological detection capabilities across Federal, State, local, and tribal governments and the private sector for a managed, coordinated response. This directive supports and enhances the effective sharing and use of appropriate information generated by the intelligence community, law enforcement agencies, counterterrorism community, other government agencies, and foreign governments, as well as providing appropriate information to these entities.

HSPD-15: War on Terror (March 2006)

HSPD-15 is classified. The objective of the directive is to improve government coordination in the global war on terror.

HSPD-16: Aviation Security Policy (June 2006)

HSPD-16 details a strategic vision for aviation security while recognizing ongoing efforts, and directs the production of a National Strategy for Aviation Security and supporting plans. The supporting plans address the following areas: aviation transportation system security; aviation operational threat response; aviation transportation system recovery; air domain surveillance and intelligence integration; domestic outreach; and international outreach. The strategy: sets forth U.S. Government agency roles and responsibilities; establishes planning and operations coordination requirements; and builds on current strategies, tools, and resources.

HSPD-17: Nuclear Materials Information Program (August 2006)

HSPD-17 is classified. The directive addresses an interagency effort managed by the Department of Energy to consolidate information from all sources pertaining to worldwide nuclear materials holdings and their security status into an integrated and continuously updated information management system.

HSPD-18: Medical Countermeasures Against Weapons of Mass Destruction (January 2007)

HSPD-18 builds on the vision and objectives articulated in the National Strategy to Combat Weapons of Mass Destruction and Biodefense for the 21st Century to ensure that the Nation's medical countermeasures research, development, and acquisitions efforts: target threats that pose the potential for a catastrophic impact on public health; yield a rapidly deployable and flexible capability to address existing and evolving threats; are part of an integrated WMD consequence management approach; and include the development of effective, feasible, and pragmatic concepts of operation for responding to and recovering from an attack. The directive designates the Secretary of Homeland Security to develop a strategic, integrated chemical, biological, radiological, and nuclear risk assessment that integrates the findings of the intelligence and law enforcement communities with input from the scientific, medical, and public health communities.

HSPD-19: Combating Terrorist Use of Explosives in the United States (February 2007)

HSPD-19 establishes a national policy and calls for the development of a national strategy and implementation plan on the prevention and detection of, protection against, and response to terrorist use of explosives in the United States. This directive mandates that the Secretary of Homeland Security coordinate with other Federal agencies to maintain secure information-sharing systems available to law enforcement agencies and other first-responders, to include best practices to enhance preparedness across governmental entities. The Secretary of Homeland Security is also responsible, in coordination with other Federal agencies, for Federal Government research, development, testing, and evaluation activities related to explosives attacks and the development of explosive render-safe tools and technologies.

HSPD-20: National Continuity Policy (May 2007)

HSPD-20 (also NSPD-51) establishes a comprehensive national policy on the continuity of Federal Government structures and operations, and designates a single National Continuity Coordinator who is responsible for leading the development and implementation of Federal continuity policies. This policy: establishes National Essential Functions; prescribes continuity requirements for all executive departments and agencies; and provides guidance for State, local, tribal, and territorial governments, and private sector organizations. This directive aims to ensure a comprehensive and integrated national continuity program that

will enhance the credibility of our national security posture and enable a more rapid and effective response to and recovery from a national emergency.

HSPD-21: Public Health and Medical Preparedness (October 2007)

HSPD-21 establishes a National Strategy for Public Health and Medical Preparedness. The Strategy draws key principles from the National Strategy for Homeland Security (October 2007), the National Strategy to Combat Weapons of Mass Destruction (December 2002), and Biodefense for the 21st Century (April 2004) that can be generally applied to public health and medical preparedness. Implementation of this strategy will transform our national approach to protecting the health of the American people against all disasters.

HSPD-22: Domestic Chemical Defense

HSPD-22 is classified. HSPD-22 establishes a national policy and directs actions to strengthen the ability of the United States to prevent, protect, respond to, and recover from terrorist attacks employing toxic chemicals and other chemical incidents.

HSPD-23: Cyber Security and Monitoring (January 2008)

HSPD-23 (also National Security Presidential Directive 54) formalizes the “Comprehensive National Cybersecurity Initiative” and a series of continuous efforts designed to establish a frontline defense (reducing current vulnerabilities and preventing intrusions), defend against the full spectrum of threats by using intelligence and strengthening supply chain security, and shape the future environment by enhancing our research, development, and education, as well as investing in leap-ahead technologies. The contents of HSPD-23 are classified.

HSPD-24: Biometrics for Identification and Screening to Enhance National Security (June 2008)

HSPD-24 establishes a framework to ensure that Federal executive departments and agencies use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information on individuals in a lawful and appropriate manner, while respecting their information privacy and other legal rights under U.S. law.

2.4 Other Authorities

Executive Order 13231, Critical Infrastructure Protection in the Information Age (October 2001) (amended by E.O. 13286, February 28, 2003)

Executive Order 13231 provides specific policy direction to ensure the protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems. It recognizes the important role that networked information systems (critical information infrastructure) play in supporting all aspects of our civil society and economy, and the increasing degree to which other critical infrastructure sectors have become dependent on such systems. It formally establishes as U.S. policy the need to protect against disruption of the operation of these systems and to ensure that any disruptions that do occur are infrequent, of minimal duration, manageable, and cause the least damage possible. This Executive Order specifically calls for the implementation of the policy to include “a voluntary public-private partnership, involving corporate and nongovernmental organizations.” This Executive Order also reaffirms existing authorities and responsibilities assigned to various executive branch agencies and interagency committees to ensure the security and integrity of Federal information systems generally and of national security information systems in particular.

National Infrastructure Advisory Council

In addition to the foregoing, Executive Order 13231 (as amended by E.O. 13286 of February 28, 2003, and E.O. 13385 of September 29, 2005) also established the NIAC as the President’s principal advisory panel on CIKR protection issues spanning all sectors. The NIAC is composed of not more than 30 members, appointed by the President, who are selected from the private sector, academia, and State and local governments, representing senior executive leadership expertise from the CIKR areas as delineated in HSPD-7.

The NIAC provides the President, through the Secretary of Homeland Security, with advice on the security of CIKR, both physical and cyber, that supports important sectors of the economy. It also has the authority to provide advice directly to the heads of other departments who have shared responsibility for CIKR protection, including HHS, DOT, and DOE. The NIAC is charged to improve the cooperation and partnership between the public and private sectors in securing critical infrastructure and advises on policies and strategies that range from risk assessment and management, to information sharing, to protective strategies and clarification of the roles and responsibilities between public and private sectors.

Executive Order 12382, President's National Security Telecommunications Advisory Committee (amended by E.O. 13286, February 28, 2003)

Executive Order 12382 creates the NSTAC, which provides to the President, through the Secretary of Homeland Security, information and advice from the perspective of the telecommunications industry with respect to the implementation of the National Security Telecommunications Policy.

Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions (amended by E.O. 13286, February 28, 2003)

Executive Order 12472 assigns NS/EP telecommunications functions, including wartime and non-wartime emergency functions, to the National Security Council, OSTP, Homeland Security Council, OMB, and other Federal agencies. This Executive Order seeks to ensure that the Federal Government has telecommunications services that will function under all conditions, including emergency situations. This Executive Order directs the NCS to assist the President, the National Security Council, the Homeland Security Council, the Director of OSTP, and the Director of the OMB in: (1) exercising the telecommunications functions and responsibilities set forth in the Executive Order; and (2) coordinating the planning for and provision of NS/EP communications for the Federal Government under all circumstances, including a crisis or emergency, an attack, recovery, and reconstitution.

Executive Order 12977, Interagency Security Committee (amended by E.O. 13286, February 28, 2003)

Executive Order 12977 directs the Interagency Security Committee to develop standards, policies, and best practices for enhancing the quality and effectiveness of physical security and the protection of nonmilitary Federal facilities in the United States. The Interagency Security Committee provides a permanent body to address continuing government-wide security for Federal facilities.

Appendix 3: The Protection Program

Appendix 3A: NIPP Core Criteria for Risk Assessments

The NIPP core criteria for risk assessments identify the characteristics and information needed to produce results that can contribute to cross-sector risk comparisons. This appendix provides information for developing new and modifying existing methodologies so they can be used to support national-level comparative risk assessment, incident response planning, resource prioritization, and protective measures development and implementation. This appendix summarizes the information provided in section 3.3, which can be referenced for additional details on these topics.

Many stakeholders conduct risk assessments to meet their own decisionmaking needs, using a broad range of methodologies. Whenever possible, DHS seeks to use information from stakeholders' assessments to contribute to an understanding of risks across sectors and regions throughout the Nation. To do this consistently, the challenge of minimizing the disparity in the approaches must be addressed through the core criteria identified below. These criteria include both the analytic principles that are broadly applicable to all parts of a risk methodology and specific guidance regarding the information needed to understand and address each of the three components of the risk equation: consequence, vulnerability, and threat.

The basic analytic principles ensure that risk assessments are:

- **Documented:** The methodology and the assessment must clearly document which information is used and how it is synthesized to generate a risk estimate. Any assumptions, weighting factors, and subjective judgments need to be transparent to the user of the methodology, its audience, and others who are expected to use the results. The types of decisions that the risk assessment is designed to support and the timeframe of the assessment (e.g., current conditions versus future operations) should be given.
- **Reproducible:** The methodology must produce comparable, repeatable results, even though assessments of different CIKR will be performed by different analysts or teams of analysts. It must minimize the number and impact of subjective judgments, leaving policy and value judgments to be applied by decisionmakers.
- **Defensible:** The risk methodology must be technically sound, making appropriate use of the professional disciplines relevant to the analysis, as well as be free from significant errors or omissions. The uncertainty associated with consequence estimates and confidence in the vulnerability and threat estimates must be communicated.

- **Complete:** The methodology must assess consequence, vulnerability, and threat for every defined risk scenario and follow the more specific guidance for each of these as given below.

Core Criteria Guidance for Consequence Assessments

- Document the scenarios assessed, tools used, and any key assumptions made.
- Estimate the number of fatalities, injuries, and illnesses, where applicable and feasible, keeping each separate estimate visible to the user.
- Estimate the economic loss in dollars, stating which costs are included (e.g., property damage losses, lost revenue, loss to the economy) and what duration was considered.
- If monetizing the human health consequences, document the value(s) used and the assumptions made.
- Consider and document any protective or consequence mitigation measures that have their effect after the incident has occurred, such as the rerouting of systems or HAZMAT or fire and rescue response.
- Describe the psychological impacts and mission disruption, where feasible.²⁴

Core Criteria Guidance for Vulnerability Assessments

- Identify the vulnerabilities associated with: physical, cyber, or human factors (openness to both insider and outsider threats); critical dependencies; and physical proximity to hazards.
- Describe all protective measures in place and how they reduce the vulnerability for each scenario.
- In evaluating security vulnerabilities, develop estimates of the likelihood of an adversary's success for each attack scenario.
- For natural hazards, estimate the likelihood that an incident would cause harm to the asset, system, or network, given that the natural hazard event occurs at the location of interest for the risk scenario.

Core Criteria Guidance for Threat Assessments

- For adversary-specific threat assessments:²⁵
 - Account for the adversary's ability to recognize the target and the deterrence value of existing security measures.
 - Identify attack methods that may be employed.
 - Consider the level of capability that an adversary demonstrates with regard to a particular attack method.
 - Consider the degree of the adversary's intent to attack the target.
 - Estimate threat as the likelihood that the adversary would attempt a given attack method against the target.
 - If threat likelihoods cannot be estimated, use conditional risk values (consequence times vulnerability) and conduct sensitivity analyses to determine how likely the scenario would have to be to support the decision.
- For natural disasters and accidental hazards:
 - Use best-available analytic tools and historical data to estimate the likelihood that these events would affect CIKR.

In addition to the guidance available in the NIPP, and as resources allow, DHS provides direct assistance to partners who are developing and modifying risk methodologies. To discuss the possibility of such assistance, contact DHS at NIPP@dhs.gov.

²⁴ The assessment of the psychological impacts and mission disruption are currently maturing capabilities. Mission disruption is an area of strong NIPP partner interest for collaborative development of the appropriate metrics to help quantify and compare different types of losses. While development is ongoing, qualitative descriptions of the consequences are a sufficient goal.

²⁵ Threat information can be received through HSIN.

Appendix 3B: Existing CIKR Protection Programs and Initiatives

This appendix provides examples of the Federal programs that currently support NIPP implementation. The examples provided herein generally cut across sectors and have national significance. These Federal programs augment the extensive State, local, tribal, territorial, and private sector protection programs that constitute important efforts already being implemented in support of the NIPP. The SSPs address sector-specific programs that are conducted under the leadership of the SSAs, and include selected protection programs undertaken by other CIKR partners that are applicable across the sector.

3B.1 Programs and Initiatives

Site Assistance Visits (SAVs): SAVs are facility vulnerability assessments jointly conducted by DHS in coordination and collaboration with Federal, State, and local stakeholders, and CIKR owners and operators. The SAV uses a hybrid methodology of dynamic and static vulnerabilities, including elements of asset-based approaches (identifying and discussing critical site assets and current CIKR protection postures) and scenario-based approaches (assault planning and likely attack scenarios) to ensure that current threats are included. Through SAVs, DHS advises CIKR owners and operators about vulnerabilities, provides recommended protective measures that would increase the ability to deter or prevent terrorist attacks, and provides recommendations for reducing vulnerabilities or enhancing resiliency. An SAV can range from a “quick look” visit to a full security vulnerability assessment that takes 3 to 5 days to comprehensively review physical, cyber, and system interdependencies.

Buffer Zone Protection Program (BZPP): The BZPP is a DHS-administered grant program designed to increase security in the “buffer zone” (the area outside of a facility that can be leveraged by an adversary to conduct target surveillance or launch an attack). The BZP is a strategic document that is developed by the responsible local law enforcement jurisdictions that identifies significant aspects of the site that may be targeted by terrorists, identifies specific threats and vulnerabilities associated with the site, and develops an appropriate buffer zone extending outward from the facility in which protective measures can be employed to make it more difficult for terrorists to conduct site surveillance or launch attacks.

Comprehensive Reviews (CRs): The CR is a cooperative government-led assessment of CIKR facilities. The CR considers not only potential terrorist methods of attack, the consequences of such an attack, integrated preparedness and response capabilities of the owner/operator, LLE, and emergency response organizations, but also preparedness and response in the context of a natural disaster. The results are used to enhance the overall security and preparedness posture of the facilities, their surrounding communities, the geographic region, and ultimately the Nation. The CR provides a forum for candid and open dialogue among all levels of government and private sector. The CR incorporates a variety of assessment and exercise tools. Information obtained from the CR is used not only to enhance the capabilities of CIKR owner/operators and community first-responders, but also to provide risk data to inform Federal investment and R&D decisions.

Characteristics and Common Vulnerabilities, Potential Indicators of Terrorist Activity, and Protective Measures Reports: These reports identify common vulnerabilities by asset class within the sectors, as well as the types of terrorist activities that are likely to be successful in exploiting these vulnerabilities. They also identify security and preparedness best practices by asset class within the sectors. Integrated Infrastructure Papers integrate these reports and are currently available to more than 500 Federal, State, local, and private sector partners on a secure Web site.

Computer-Based Assessment Tool (CBAT): CBAT is an extension of the technical assistance provided for the DHS SAV Program and BZPP and is in support of designated special events. CBAT comprises technology and services that help DHS, owners and operators, local law enforcement, and emergency personnel prepare for, respond to, and manage special events. By integrating SAV and BZPP assessment data with geospherical video and geospatial and hypermedia data, CBAT provides planners with a computer-based, cross-platform tool that allows them to present data, make informed decisions quickly, and confidently respond to an incident. The “video walkthrough” of the facility or perimeter provided by CBAT also gives emergency response personnel a view of what they will encounter onsite. The system combines six individual, high-resolution cameras that provide a 360-degree spherical color video of the facilities, routes, and specific areas pertaining to a CBAT request.

Control Systems Security Initiative: DHS sponsors programs to increase the security of Internet-based control systems. A control system comprises components (designed to maintain the operation of a process or system) that are connected or related in such a manner as to command, monitor, direct, or regulate itself or another system. Control systems are embedded throughout the Nation’s CIKR and may be increasingly vulnerable to cyber threats that could have a devastating impact. The DHS Control Systems Security Initiative provides coordination among Federal, State, local, and tribal governments, as well as control system owners, operators, and vendors to improve control system security within and across all CIKR sectors.

Federal Cyber System Security Programs: DHS established the GFIRST to facilitate interagency information sharing and cooperation across the Federal agencies responsible for cyber system readiness and response. GFIRST members work together to understand and manage computer security incidents and encourage proactive and preventive security practices. Other examples of Federal agency cybersecurity access control, certification, and policy enforcement tools include:

- The General Services Administration (GSA) is responsible for developing and implementing an infrastructure for authentication services, as well as an automated risk assessment tool for government-wide use in certifying and accrediting its eAuthentication gateway. GSA is creating a list of approved solution providers that supply smart cards based on Federal Public Key Infrastructure standards and that include a new electronic authentication policy specification.
- The National Oceanic and Atmospheric Administration (NOAA) has implemented enterprise-wide vulnerability assessments and virus-detection software, an intrusion-detection system, anti-virus scanning gateways, and a patch management policy.

Federal Hazard Mitigation Programs: FEMA administers three programs that provide funds for activities that reduce the losses from future disasters or help prevent the occurrence of catastrophes. These hazard mitigation programs include the Flood Mitigation Assistance Program, the Hazard Mitigation Grant Program, and the Pre-Disaster Mitigation Program. These programs enable grant recipients to undertake activities such as the elevation of structures in floodplains, the relocation of structures from floodplains, the construction of structural enhancements to facilities and buildings in earthquake-prone areas (also known as retrofitting), and modifications to land-use plans to ensure that future construction ameliorates hazardous conditions.

International Outreach Program: DHS works with DOS and other CIKR partners to conduct international outreach with foreign countries and international organizations to encourage the promotion and adoption of best practices, training, and other

programs, as needed, to improve the protection of overseas assets and to help ensure the reliability of the foreign infrastructure on which the United States depends.

National Cyber Exercises: DHS conducts exercises to identify, test, and improve coordination of the cyber incident response community, including Federal, State, local, tribal, territorial, and international governmental entities, as well as private sector corporations and coordinating councils.

National Cyber Response Coordination Group (NCRCG): This entity facilitates coordination of the Federal Government's efforts to prepare for, respond to, and recover from cyber incidents and physical attacks that have significant cyber consequences (collectively known as "cyber incidents"). The NCRCG serves as the Federal Government's principal interagency mechanism for operational information sharing and coordination of the Federal Government's response and recovery efforts during a cyber crisis. It uses established relationships with the private sector and State and local governments to help manage a cyber crisis, develop courses of action, and devise appropriate response and recovery strategies.

Protective Security Advisor (PSA) Program: DHS protection specialists are assigned as liaisons between DHS and the protective community at the State, local, and private sector levels in geographical areas representing major concentrations of CIKR across the United States. The PSAs are responsible for sharing risk information and providing technical assistance to local law enforcement and CIKR owners and operators of CIKR within those areas. They also serve an important role in facilitating the CIKR-related aspects of incident management operations under the NRF.

Software Assurance: DHS is developing best practices and new technologies to promote integrity, security, and reliability in software development. Focused on shifting away from the current security paradigm of patch management, DHS is leading the Software Assurance Program, a comprehensive strategy that addresses processes, technology, and acquisition throughout the software life cycle to result in secure and reliable software that supports critical mission requirements.

3B.2 Guidelines, Reports, and Planning

Cybersecurity Planning: DHS recognizes that each sector will have a unique reliance on cyber systems and will, therefore, assist SSAs in considering a range of effective and appropriate cyber protective measures. The sector-level approaches to cybersecurity will be documented in the respective SSPs.

Educational Reports: DHS provides several types of informational reports to support efforts to protect CIKR. They cover subjects such as CIKR common vulnerabilities, potential indicators of terrorist activity, and best practices for protective measures. As they are developed, these reports are distributed to all State and Territorial Homeland Security Offices with the guidance that they should be shared with CIKR owners and operators, the law enforcement community, and captains of the ports in their respective jurisdictions.

Risk Management Manuals: In response to the September 11, 2001 attacks, FEMA's role was expanded to include activities to reduce the vulnerability of buildings to terrorist attacks. In support of this mission, FEMA created the Risk Management Series, a collection of publications directed toward providing design guidance to mitigate the consequences of manmade disasters.

To date, the series includes the following manuals:

- FEMA 155, Building Design for Homeland Security
- FEMA 426, Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings
- FEMA 427, Primer for the Design of Commercial Buildings to Mitigate Terrorist Attacks
- FEMA 428, Primer to Design Safe School Projects in Case of Terrorist Attacks
- FEMA 429, Insurance, Finance, and Regulation Primer for Terrorism Risk Management in Buildings
- FEMA 430, Primer for Incorporating Building Security Components in Architectural Design
- FEMA 452, Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings
- FEMA 453, Multihazard Shelter (Safe Havens) Design

3B.3 Information-Sharing Programs That Support CIKR Protection

Federal agencies and the law enforcement community provide information-sharing services and programs that support CIKR protection information sharing. These include:

- **DHS Homeland Security Information Network (HSIN):** HSIN is a national, Web-based communications platform that allows: DHS; SSAs; State, local, tribal, and territorial governmental entities; and other partners to obtain, analyze, and share information based on a common operating picture of strategic risk and the evolving incident landscape. The network is designed to provide a robust, dynamic information-sharing capability that supports both NIPP-related steady-state CIKR protection and NRF-related incident management activities, and to provide the information-sharing processes that form the bridge between these two homeland security missions. HSIN is one part of the ISE called for by the Intelligence Reform and Terrorism Prevention Act of 2004. As specified in the act, it will provide users with access to terrorism information that is matched to their roles, responsibilities, and missions in a timely and responsive manner. HSIN is discussed in detail in chapter 4. HSIN-Critical Sectors is an information-sharing portal designed to encourage communication and collaboration among all CIKR sectors and the Federal government. The content is tailored for each of the CIKR sectors.
- **FBI's InfraGard:** InfraGard is an information-sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the FBI and the private sector. InfraGard is an association of businesses, academic institutions, State and local law enforcement agencies, and other participants dedicated to sharing information and intelligence related to the protection of U.S. CIKR from both physical and cyber threats. InfraGard chapters are geographically linked with FBI Field Offices. Each InfraGard chapter has an FBI Special Agent Coordinator who works closely with Supervisory Special Agent Program Managers in the Cyber Division at FBI Headquarters.
- **Interagency Cybersecurity Efforts:** Interagency cooperation and information sharing are essential to improving national counterintelligence and law enforcement capabilities pertaining to cybersecurity. The intelligence and law enforcement communities have various official and unofficial information-sharing mechanisms in place. Examples include:
 - *U.S. Secret Service's Electronic Crimes Task Forces (ECTFs):* These ECTFs provide interagency coordination on cyber-based attacks and intrusions. At present, 15 ECTFs are in operation, with an expansion planned.
 - *FBI's Inter-Agency Coordination Cell:* The Inter-Agency Coordination Cell is a multi-agency group focused on sharing law enforcement information on cyber-related investigations.
 - *Computer Crime and Intellectual Property Section:* The DOJ, Criminal Division, Computer Crime and Intellectual Property Section is responsible for prosecuting nationally significant cases of cyber crime and intellectual property crime. In addition to its direct litigation responsibilities, the division formulates and implements criminal enforcement policy and provides advice and assistance.
- **Law Enforcement Online (LEO):** The FBI provides LEO as a national focal point for electronic communications, education, and information sharing for the law enforcement community. LEO, which can be accessed by any approved employee of a Federal, State, or local law enforcement agency, or approved member of an authorized law enforcement special interest group, is intended to provide a communications mechanism to link all levels of law enforcement throughout the United States.
- **Regional Information Sharing Systems (RISS):** The RISS program is a federally funded program administered by the DOJ, Office of Justice Programs, Bureau of Justice Assistance. RISS serves more than 8,100 member law enforcement agencies in 50 States, the District of Columbia, Guam, Puerto Rico, the U.S. Virgin Islands, Australia, Canada, and the United Kingdom. The program comprises six regional centers that share intelligence and coordinate efforts against criminal networks that operate in many locations across jurisdictional lines. Typical targets of RISS activities are terrorism, drug trafficking, violent crime, cyber crime, gang activity, and organized criminal activities. The majority of the member agencies are at the municipal and county levels; however, more than 485 State agencies and more than 920 Federal agencies also participate. The Drug Enforcement Administration; FBI; U.S. Attorneys' Offices; Internal Revenue Service; Secret Service; U.S. Immigration and Customs Enforcement; and the Bureau of Alcohol, Tobacco, Firearms, and Explosives are among the Federal agencies participating in the RISS program.

- **Sharing National Security Information:** The ability to share relevant classified information poses a number of challenges, particularly when the majority of industry facilities are neither designed for nor accredited to receive, store, and dispose of these materials. Ultimately, HSIN may be used to more efficiently share appropriate classified national security information with cleared private sector owners and operators during incidents, times of heightened threat, or on an as-needed basis. While supporting technologies and policies are identified to satisfy this requirement, DHS will continue to expand its initiative to sponsor security clearances for designated private sector owners and operators, sharing classified information using currently available methods.
- **Web-Based Services for Citizens:** A variety of Web-based information services are available to enhance the general awareness and preparedness of American citizens. These include CitizenCorps.gov, FirstGov.gov, Ready.gov, and USAonwatch.org.



Appendix 3C: Infrastructure Data Warehouse

3C.1 Why Do We Need a National CIKR Inventory?

HSPD-7 directs the Secretary of Homeland Security to lead efforts to reduce the Nation's vulnerability to terrorism and deny the use of infrastructure as a weapon by developing, coordinating, integrating, and implementing plans and programs that identify, catalog, prioritize, and protect CIKR in cooperation with all levels of government and private sector entities. A central Federal data repository for analysis and integration is required to provide DHS with the capability to identify, collect, catalog, and maintain a national inventory of information on assets, systems, and networks that may be critical to the Nation's well-being, economy, and security. This inventory is also essential to help inform decisionmaking and specific response and recovery activities pertaining to natural disasters and other emergencies.

To fulfill this need, DHS has developed the federated IDW, a continually evolving and comprehensive catalog of the assets, systems, and networks that make up the Nation's CIKR. The IDW enables access to descriptive information regarding CIKR. Although the IDW is not a listing of prioritized assets, it has the capability to help inform risk-mitigation activities across the CIKR sectors and government jurisdictions.

3C.2 How Does the Inventory Support the NIPP?

The IDW provides a coordinated and consistent framework to access and display the CIKR data submitted by: Federal, State, and local agencies; the private sector; and integrated Federal or commercial databases. The federated framework and structure of the IDW have been constructed to readily integrate other CIKR data sources and provide the required data in a usable and effective manner. Two primary components of this framework are the Infrastructure Protection Taxonomy and infrastructure type data fields:

- The IP taxonomy groups CIKR by sector and identifies overlaps between and across sectors. It was developed by DHS in coordination with the SSAs to ensure that every CIKR type is represented.

- The infrastructure type data fields outline the attributes of interest that are integral to assessment and analysis per a specific category of CIKR, making the IDW compliant with the National Information Exchange Model (NIEM). The information contained in these data fields feeds the strategic risk assessment process used to prioritize CIKR in the context of terrorist threats or incidents, natural disasters, or other emergencies.

The information accessed through the IDW supports the analysis to determine which assets, systems, and networks make up the Nation’s CIKR and to inform security planning and preparedness, resource investments, and post-incident response and recovery activities within and across sectors and governmental jurisdictions.

3C.3 What Is the Current Content of the Inventory?

DHS gathers data related to the Nation’s CIKR from a variety of sources. The inventory reflects a collection of information garnered from formal data calls, voluntary additions, and the leveraging of various Federal and commercial databases. Information accessed through the IDW has been received from Federal agencies, State and local submissions, voluntary private sector submissions, commercial demographics products, external data sources, and subject matter experts. The information is used to inform CIKR protection efforts, contingency planning, and planning for implementation of initiatives such as the BZPP, and to aid decisionmakers during response and recovery following terrorist attacks, natural disasters, or other emergencies.

3C.4 How Will the Current Inventory Remain Accurate?

DHS continues to seek input from multiple infrastructure sources, including existing databases managed by SSAs, commercial providers, State and local governments, and the private sector. Integrating existing databases using a federated framework will provide a dynamic common operating interface of infrastructure and vulnerability information through a cross-flow of data between separate databases or linked access to other databases. Existing databases being considered for integration are shown in table 3C-1. Ownership and control of the data will be determined according to the circumstances of each database. Classification of the data will be based on Original Classification Authority (OCA) guidance and will be protected as required by OCA guidance and direction.

Table 3C-1: Database Integration

Database	Use
Integrated Common Analytical Viewer (ICAV)	DHS is leveraging existing geospatial capabilities and technology used by the National Geospatial-Intelligence Agency by implementing the iCAV as a DHS Geospatial Enterprise Solution for geospatial mapping, analysis, and sorting of the Nation’s CIKR. The iCAV system will use the geospatial component to spatially display and map CIKR information.
National Threat Incident Database	This database provides a source of consolidated information concerning credible threats and incidents related to our Nation’s CIKR.
DHS LENS Vulnerability Databases	These databases contain Characteristics and Common Vulnerabilities and Potential Indicators of Terrorist Activity Reports, and Site Assistance Visits and BZPP schedules. Site Assistance Visits and BZPP documents will be available through classified and unclassified secure portals as applicable.
Commercial/Sector-Specific Databases	Many existing Federal and commercial databases contain information sets pertinent to the CIKR mission. Commercial databases will be purchased based on available funding and priorities for information requirements.

3C.5 How Will the Infrastructure Data Warehouse Be Maintained?

The process of ensuring that the data collected is both current and accurate is continual. Data updates and currency are largely dependent on the sources of the data and the frequency of the updates that they provide.

Efficiency and reliability are maintained through the implementation of various data quality control techniques. Verification and validation efforts by contracted companies or Federal employees will play a key role in ensuring information currency.

3C.6 How Do CIKR Partners Contribute?

The CIKR information accessible through the IDW is highly dependent on the participation and support of the SSAs, the States, and private sector entities:

- SSAs have the primary responsibility for providing sector information to DHS for inclusion in the IDW.²⁶ The processes used for sector CIKR and database identification in coordination with partners should be described in the SSPs.
- Some State governments have either already developed infrastructure databases or have begun the process to identify and assess CIKR within their jurisdictions. State Homeland Security Advisors should work closely with DHS and the SSAs to ensure that data collection efforts are streamlined, coordinated, and reflect the most accurate data possible.
- The most current and accurate data are best known by CIKR owners and operators. Thus, as the owners and operators of the majority of the Nation's CIKR, private sector entities are encouraged to be actively involved in the development of CIKR information.

3C.7 What Are the Plans for IDW Expansion?

Planned advancements include integration with multiple commercial and Federal CIKR databases, vulnerability assessment tools and libraries, intelligence and threat reporting databases, and geospatial tools.

DHS is developing the IDW with a versatile platform to support integration of DHS and SSA applications and databases. The goal of this effort is to create a means for appropriate parties to access national CIKR information that more efficiently and effectively supports the implementation of NIPP risk management framework activities, including:

- Integration of vulnerability, consequence, and asset/system/network attribute data into a single portal interface as the foundation for the NIPP risk assessment process;
- Access to threat data to support the development of asset, system, and network risk scores;
- Assessment and, if appropriate, prioritization of assets, systems, and networks across sectors and jurisdictions based on risk to promote the more effective allocation and use of available resources and to inform planning, threat response, and post-incident restoration actions at all levels of government and the private sector;
- Sharing of consistent information so that all partners involved in CIKR protection operate from a common frame of reference;
- Acting as a primary information and integration hub for protective security needs throughout the country in support of DHS- and SSA-led activities;
- Supporting the efforts of law enforcement agencies during National Security Special Events and other high-priority security events; and
- Supporting the efforts of primary Federal agencies in responding to and recovering from major natural or manmade disasters.

²⁶ The IP Taxonomy is the foundation for multiple DHS programs that focus on CIKR, such as the IDW and the National Threat Incident Database, and should provide the foundation for the lexicon used in the SSPs. This common framework will allow more efficient integration and transfer of information, as well as a more effective analytical tool for making comparisons.



Appendix 4: Existing Coordination Mechanisms

The coordination mechanisms established under the NIPP serve as the primary means for coordinating CIKR protection activities nationally. However, many other avenues exist for CIKR partners to engage with each other and government at all levels to ensure that their efforts are fully coordinated in accordance with the principles outlined in the NIPP. The following table summarizes many of these available mechanisms.

Coordination	Mechanism	Description
Local to Local	Interlocal Agreements	Cities and towns exchange information and cooperate on any number of projects. Interlocal agreements are a mechanism to do cooperatively anything that can be done as an individual municipality.
	Mutual-Aid Agreements	Established means through which one local government can offer assistance and another can receive assistance at a time of disaster. These agreements cover logistics, deployment, liability, reimbursement, and many other issues. The intent is to provide assistance in the most efficient manner possible by coordinating the relevant terms and conditions in advance.
	County Commissioner Interaction	County commissioners provide leadership, services, and programs to meet the health, safety, and welfare needs of their citizens in an integrated, collaborative network.
Local to State	Committees, Commissions, and Boards	Local-to-State legislative- and regulatory-level interactions occur through State committees, commissions, and boards dealing with counterterrorism, environmental, transportation, community development, retirement, insurance, and many other issues. Interactions also include coordination among the Office of the Governor, the Homeland Security Advisor, the Emergency Management Agency, and the National Guard.
Local to Federal	Associations	National associations of local governments serve as a bridge between local elected officials and the Federal Government to ensure that the public safety and homeland security needs of the localities are met. These organizations, such as the National League of Cities, the National Association of Counties, and the U.S. Conference of Mayors, work to ensure that Federal resources are appropriately targeted for disaster planning, mitigation, and recovery.
State to State	Intrastate Councils of Government	Councils of State Governments are regional councils that, by law, are political subdivisions of the State with the authority to plan and initiate needed cooperative projects; however, they do not have the power to regulate or tax because these authorities are exclusively assigned to cities and counties. A council's duties may include comprehensive planning for regional employment and training needs, criminal justice, economic development, homeland security, emergency preparedness, bioterrorism, 911 service, solid waste, aging, transportation, rural development, and various other needs.
	Interstate or Regional Compacts (including those with cross-border entities)	<p>States face issues that are not confined to geographical boundaries or jurisdictional lines. Interstate compacts are a mechanism that can be used to address sector interdependencies and coordinate protection of CIKR. Compacts are organized in a number of ways:</p> <ul style="list-style-type: none"> • Sector-based compacts focus on specific CIKR resources that are shared or are interdependent across State boundaries (e.g., the Western Interstate Energy Compact). • Preparedness-focused compacts, such as the Interstate Mutual-Aid Compact, establish a means for participating jurisdictions to provide voluntary assistance to other States in response to an event that overwhelms the resources of individual State and local governments. • Regional compacts provide a means for participating jurisdictions to coordinate activities within a specific geographical area that spans multiple States. These agreements, such as the Canadian River Compact, define the specific equities of each State within the particular region. <p>For more information on interstate compacts, contact the National Center for Interstate Compacts through their Web site at www.csg.org/programs/ncic/default.aspx.</p>

Coordination	Mechanism	Description
State to Federal	Associations	Organizations such as the National Governors Association, the National Conference of State Legislatures, and the Council of State Governments represent the interests of the States in the Federal policymaking process. State-level professional associations, such as the Association of State Drinking Water Administrators and the Association of State and Interstate Water Pollution Control Administrators, also provide sector-specific coordination mechanisms; there are similar associations for each of the sectors. Additionally, these groups support State leaders by keeping their members informed of key Federal decisions that affect State government.
	State Liaison Offices	Some States have formed specific liaison offices in Washington, DC, to maintain awareness of Federal developments and to ensure that their individual State's perspective is represented in the Federal policymaking process. These offices report back regularly to their State's leadership and legislature regarding Federal issues of interest.
	State and Local Fusion Centers (SLFCs)	The DHS Office of Intelligence and Analysis (I&A) places intelligence analysts in SLFCs to provide a coherent point of information exchange and intelligence sharing among the Federal Government and State, local, and tribal governments. In addition, the PSA Program is deploying field-based Protective Security Advisor Analysts to select SLFCs throughout the country. Their focus will be to analyze risks to CIKR in the region relative to current intelligence and to aid State, local, and private sector representatives in prioritizing CIKR protection efforts.
Federal to Federal	Memoranda of Understanding or Agreement	Agreements among two or more Federal departments and agencies to cooperate on a specific topic or initiative.
	Interagency Security Committee	The ISC is a permanent body of senior representatives from all branches of the government that addresses continuing government-wide security for Federal facilities.
Private Sector to Government (all levels)	Public-Private Partnerships	A public-private partnership is a contractual agreement between a public agency (i.e., Federal, State, or local) and a private sector entity. Through this agreement, the skills and assets of each sector (public and private) are shared in delivering a service or providing a facility for the use of the general public.
	Advisory Councils, Boards, and Commissions	In addition to the SCCs and ISACs, a variety of private sector organizations exist that focus on homeland security and CIKR protection activities on a sector and geographical basis. These groups are made up of members of the public and subject matter experts, and provide advice and recommendations to government at all levels.
	Associations	Myriad private sector associations exist that advocate on behalf of their members in the policymaking process at the Federal, State, and local levels. These groups are made up of individuals or companies with common interests. Because of their ability to communicate with their members, private associations provide an effective means for government to provide information to the public and also learn about the concerns of specific groups of CIKR partners. In addition, many associations serve as standard-setting organizations for their sectors.



Appendix 5: Integrating CIKR Protection as Part of the Homeland Security Mission

Appendix 5A: State, Local, Tribal, and Territorial Government Considerations

State, local, tribal, and territorial efforts support the implementation of the NIPP and associated SSPs by providing a jurisdictional focus and enabling cross-sector coordination. The NIPP recognizes that there is not a one-size-fits-all approach to CIKR protection planning at the State and local levels. Creating and managing a CIKR protection program for a given jurisdiction entails building an organizational structure and mechanisms for coordination between government and private sector entities that can be used to implement the NIPP risk management framework. This includes taking action within the jurisdiction to set goals and objectives; identify assets, systems, and networks; assess risks; prioritize CIKR across sectors; implement protective programs and resiliency strategies; and measure the effectiveness of risk-mitigation efforts. These elements form the basis of CIKR protection programs and guide the implementation of relevant CIKR protection-related goals and objectives outlined in State, local, tribal, and territorial homeland security strategies.

This appendix provides general guidance that can be tailored to: unique jurisdictional characteristics; organizational structures; and operating environments at the State, local, tribal, and territorial levels. Additional guidance is available in *A Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal, and Territorial Levels* (2008). This guide can be accessed at www.dhs.gov/nipp.

The NIPP is structured to avoid redundancy and to ensure coordination among Federal, State, and local CIKR protection efforts. States or localities are encouraged to focus their efforts in ways that leverage Federal resources and address the relevant CIKR sector's protection requirements in their particular areas or jurisdictions. This appendix outlines a basic framework to guide the development of CIKR protection strategies, plans, and programs in coordination with the NIPP.

To be in alignment with the NIPP, State and local CIKR protection plans and programs should explicitly address six broad categories:

- CIKR protection roles and responsibilities;
- Partnership building and information sharing;
- Implementation of the NIPP risk management framework;
- CIKR data use and protection;

- Leveraging of ongoing emergency preparedness activities for CIKR protection; and
- Integration of Federal CIKR protection and resiliency activities.

5A.1 CIKR Roles and Responsibilities

The NIPP outlines a set of broad roles and responsibilities for State, local, tribal, territorial, and regional entities (see chapter 2). State, local, tribal, territorial, and regional CIKR protection plans (or entities addressing CIKR in State or local homeland security plans or strategies) should describe how each jurisdiction intends to implement these roles and responsibilities. In particular, jurisdictions should consider and describe in their plans the following:

- Which offices or organizations in the jurisdiction perform the roles or responsibilities outlined in the NIPP or the supporting SSPs;
- Whether gaps exist between the jurisdiction's current approach and those roles and responsibilities outlined in the NIPP or in an SSP, and how the gaps will be addressed;
- Whether any roles and responsibilities should be revised, modified, or consolidated to accommodate the unique operating attributes of the jurisdiction;
- How the jurisdiction will maintain operational awareness of the performance of the CIKR protection roles assigned to different offices, agencies, or localities; and
- How the jurisdiction will coordinate its CIKR protection roles and responsibilities with other jurisdictions and the Federal Government.

5A.2 Partnership Building and Information Sharing

Effective CIKR protection requires the development of partnerships, collaboration, and information sharing between government and CIKR owners and operators. This includes maintaining awareness of CIKR owner and operator concerns, disseminating relevant information to owners and operators, and maintaining processes for rapid response and decisionmaking in the event of a threat or incident involving CIKR within the jurisdiction. To address partnership building, networking, and information sharing, State and local entities should determine whether the appropriate mechanisms for sharing information and networking with CIKR partners are in place. If mechanisms are not established at all of the relevant levels, State and local entities should identify the means for better coordinating and sharing information with CIKR partners. Options to be considered and described in State, local, tribal, territorial, and regional CIKR protection plans can include, but are not limited to:

- Ensuring collaboration with other governmental entities and the private sector using a process based on the partnership model outlined under the NIPP or an abbreviated form of the model that addresses only those sectors that are most relevant to the jurisdiction;
- Instituting specific information-sharing networks, such as an information-sharing portal, for the jurisdiction. These types of networks allow owners and operators, and governmental entities to share best practices, provide a better understanding of sector and cross-sector needs, and inform collective decisionmaking on how best to utilize resources;
- Utilizing SLFCs, where applicable. SLFCs coordinate the collection, analysis, and dissemination of law enforcement, homeland security, public safety, and terrorism information;
- Developing standing committees and work groups to discuss relevant CIKR protection issues;
- Developing a regular newsletter or similar communications tool for CIKR owners and operators on relevant CIKR protection issues and coordination within the jurisdiction; and
- Participating in existing sector-wide and national information-sharing networks, including those offered by trade associations, ISACs, SCCs, and threat warning and alert notification systems.

The information-sharing approach for a given jurisdiction will vary based on CIKR ownership, the number and type of CIKR sectors represented in the jurisdiction, and the extent to which existing mechanisms can be leveraged. The options presented above are merely a description of some available mechanisms that jurisdictions may consider as they develop the organization of their programs and document their processes in a CIKR protection plan.

5A.3 Implementing the Risk Management Framework

The NIPP risk management framework described in chapter 3 provides a useful model for State, local, tribal, territorial, and regional jurisdictions to use in addressing CIKR protection within the given jurisdiction. The model provides a risk-informed approach to identify, prioritize, and protect CIKR assets and systems at the State and local level. This process also allows State and local jurisdictions to enhance coordination with DHS and the SSAs in developing and implementing CIKR protection programs. The following should be considered when developing CIKR protection programs:

- What are the jurisdiction's goals and objectives for CIKR protection? How do these goals relate to those of the NIPP and the SSPs that are relevant to the jurisdiction?
- What are the CIKR assets, systems, and networks within the jurisdiction or that affect the jurisdiction? Are there significant interstate or international dependencies or interdependencies? Are any of the assets, systems, or networks within the jurisdiction deemed to be nationally critical by DHS?
- Are risk assessments for CIKR within the State being conducted or planned by DHS, the SSAs, or owners and operators in accordance with the processes outlined in the NIPP? Is there a need for the jurisdiction to conduct additional or supplemental risk assessments? Do the methodologies for conducting risk assessments address the baseline criteria outlined in chapter 3?
- What are the CIKR protection priorities within the jurisdiction? How do these priorities correlate with the national priorities established by the Federal Government? How do these priorities correlate with the ongoing CIKR protection priorities established for each sector at the national level?
- What actions or initiatives are being taken within the jurisdiction to address CIKR protection and resiliency? How do these relate to the national effort?
- What types of metrics will be used to measure the progress of CIKR protection efforts?

5A.4 CIKR Data Use and Protection

States and other jurisdictions may employ a variety of means to collect CIKR data or respond to CIKR data requests. State, local, tribal, territorial, and regional plans should outline how the jurisdiction has organized itself to address CIKR data use and protection. The following issues should be considered in developing the CIKR protection plan:

- Will the jurisdiction maintain a comprehensive database of CIKR in the State, region, or locality? How will the jurisdiction collect such information? What tools are available from DHS or in the commercial marketplace to support infrastructure information collection and management?
- How will sensitive data that may be in the possession of State, local, tribal, or territorial governments be legally and physically protected from public disclosure and what safeguards will be used to control and limit distribution to the appropriate individuals?
- Will data collection mechanisms be compatible and interoperable with the IDW framework to enable data sharing?
- How will the jurisdiction ensure that it is maintaining current information?
- Will data requests from the Federal Government for CIKR data be channeled to the owners and operators through the States?
- Are there local legal authorities and policy directives related to data collection? Are these authorities adequate? If not, how will the jurisdiction address these issues?

5A.5 Leveraging of Ongoing Emergency Preparedness Activities for CIKR Protection

The emergency management capabilities of each State and local jurisdiction are an important component of improving overall CIKR protection. States and localities should look to existing programs and leverage ways in which CIKR protection can be integrated into ongoing activities. Areas to be considered when drafting a CIKR protection plan include:

- Does the jurisdiction's exercise program account for CIKR protection? If not, how will the State or locality incorporate CIKR protection exercise scenarios to increase the level of preparedness?
- Does the State Preparedness Report account for CIKR protection?
- How do CIKR protection efforts relate to initiatives outlined in the jurisdiction's hazard mitigation plan? How do various hazard modeling or ongoing mitigation efforts relate to the CIKR protection initiatives?
- How will the jurisdiction share best practices, reports, or other output from emergency preparedness activities with CIKR owners and operators?
- Have CIKR owners and operators been invited to participate in exercise events and are CIKR owners and operators linked to existing warning or response systems?
- What existing educational and outreach programs can be leveraged to share information with partners regarding CIKR protection?
- Are there other outreach or emergency management programs that should include a CIKR component?

5A.6 Integrating Federal CIKR Protection Activities

State-, local-, tribal-, and territorial- level CIKR protection programs should complement and draw on Federal efforts to the maximum extent possible to utilize risk management methodologies and avoid the duplication of efforts.

State, local, tribal, and territorial efforts should consider the adequacy of DHS and SSA guidance and resources for their particular situation. For example:

- Are the existing criteria for risk analysis inclusive of levels of consequence that are of concern to the State or locality, or should the jurisdiction's criteria be expanded to include additional local assets?
- Are the self-assessment tools developed by DHS and the SSAs sufficient or do these tools need additional tailoring to reflect local conditions?
- Are there additional best practices that should be shared among CIKR partners?
- Are there additional authorities that need to be documented?

Appendix 5B: Recommended Homeland Security Practices for Use by the Private Sector

This appendix provides a summary of practices that may be adopted by private sector owners and operators to improve the efficiency and effectiveness of their CIKR protection programs. The recommendations herein are based on best practices in use by various sectors and other groupings. The NIPP encourages private sector owners and operators to adopt and implement those practices that are appropriate and applicable at the enterprise and individual facility levels. These may include:

- Asset, System, and Network Identification:
 - Incorporate the NIPP framework for the assets, systems, and networks under their control; and
 - Voluntarily share CIKR-related information with the appropriate partners to facilitate CIKR protection program implementation with applicable information protections.
- Assessment, Monitoring, and Reduction of Risks/Vulnerabilities:
 - Conduct appropriate risk and vulnerability assessment activities using tools or methods that are rigorous, well-documented, and based on accepted practices in industry or government;
 - Implement measures to reduce risk and mitigate deficiencies and vulnerabilities corresponding to the physical, cyber, and human security elements of CIKR protection;
 - Maintain the tools, capabilities, and protocols necessary to provide an appropriate level of monitoring of networks, systems, or a facility and its immediate surroundings to detect possible insider and external threats;
 - Develop and implement personnel screening programs to the extent feasible for personnel working in sensitive positions; and
 - Manage the security of computer and information systems while maintaining awareness of vulnerabilities and consequences to ensure that systems are not used to enable attacks against CIKR.

- Information Sharing:

- Connect with and participate in the appropriate national, State, regional, local, and sector information-sharing mechanisms (e.g., HSIN-CS);
- Develop and maintain close working relationships with local (and, as appropriate, Federal, State, tribal, and territorial) law enforcement and first-responder organizations relevant to the company's facilities to promote communication, with the appropriate protections, and cooperation related to prevention, remediation, and response to a natural disaster or terrorist event;
- Provide applicable information on threats, assets, and vulnerabilities to appropriate government authorities, with the appropriate protections;
- Share threat and other appropriate information with other CIKR owners and operators;
- Participate in activities or initiatives developed and sponsored by the relevant NIPP SCC or entity that provides the sector coordinating function;
- Participate in, share information with (with appropriate protections), and support State and local CIKR protection programs, including coordinating and planning with Local Emergency Planning Committees and Citizen Corps²⁷ Councils;
- Collaborate with other CIKR owners and operators on security issues of mutual concern; and
- Use appropriate measures to safeguard information that could pose a threat and maintain open and effective communications regarding security measures and issues, as appropriate, with employees, suppliers, customers, government officials, and others.

- Planning and Awareness:

- Develop and exercise appropriate emergency response, mitigation, and business continuity-of-operations plans;
- Participate in Federal, State, local, or company exercises and other activities to enhance individual, organization, and sector preparedness and resiliency;
- Demonstrate a continuous commitment to security and resilience across the entire company;
- Develop an appropriate security protocol corresponding to each level of the HSAS. These plans and protocols are additive so that as the threat level increases for company facilities, the company can quickly implement its plans to enhance the physical or cybersecurity measures in operation at these facilities and modify them as the threat level decreases;
- Utilize National Fire Protection Association 1600 Standard on Disaster/Emergency Management and Business Continuity Programs, endorsed by DHS and Congress, when developing Emergency Response and Business Continuity-of-Operations Plans if the sector has not developed its own standard;
- Document the key elements of security programs, actions, and periodic reviews as part of a commitment to sustain a consistent, reliable, and comprehensive program over time;
- Enhance security awareness and capabilities through periodic training, drills, and guidance that involve all employees annually to some extent and, when appropriate, involve others such as emergency response agencies or neighboring facilities;
- Perform periodic assessments or audits to measure the effectiveness of planned physical security and cybersecurity measures. These audits and verifications should be reported directly to the CEO or his/her designee for review and action;

²⁷ The U.S. Citizen Corps is the FEMA grassroots strategy to achieve community preparedness and resilience. Local Citizen Corps Councils bring government and civic leaders from all sectors together to develop goals and strategies for community resilience tailored to specific community vulnerabilities and population. Elements of local strategies include: outreach and education on personal preparedness; integration of nongovernmental assets and personnel in preparedness and response protocols; improved plans for emergency notifications, evacuation, and sheltering; and increased citizen participation in community safety. More information is available on the Internet at www.CitizenCorps.gov.

- Promote preparedness education and outreach and emergency response training through the U.S. Citizen Corps, such as the Community Emergency Response Team training offered for employees;
- Consider including programs for developing highly secure and trustworthy operating systems in near-term acquisitions or R&D priorities;
- Participate in the Voluntary Private Sector Preparedness Accreditation and Certification Program, which establishes a common set of criteria for private sector preparedness in disaster management, emergency management, and business continuity;
- Create a culture of preparedness, reaching every level of the organization’s workforce, which ingrains in each employee the importance of awareness and empowers those with responsibilities as first-line defenders within the organization and the community;
- As the organization performs R&D or acquires new or upgraded systems, consider only those that are highly secure and trustworthy;
- Encourage employee participation in community preparedness and protection efforts, such as sector-specific Watch programs and skill-based volunteer programs, including Medical Reserve Corps, Red Cross, Second Harvest, etc.;
- Work with others locally, including government, nongovernmental organizations, and private sector entities, both within and outside of the sector, to identify and resolve gaps that could occur in the context of a terrorist incident, natural disaster, or other emergency;
- Work with DHS to improve cooperation regarding personnel screening and information protection; and
- Identify supply chain and “neighbor” issues that could cause workforce or production disruptions for the company.



Appendix 6: S&T Plans, Programs, and Research & Development

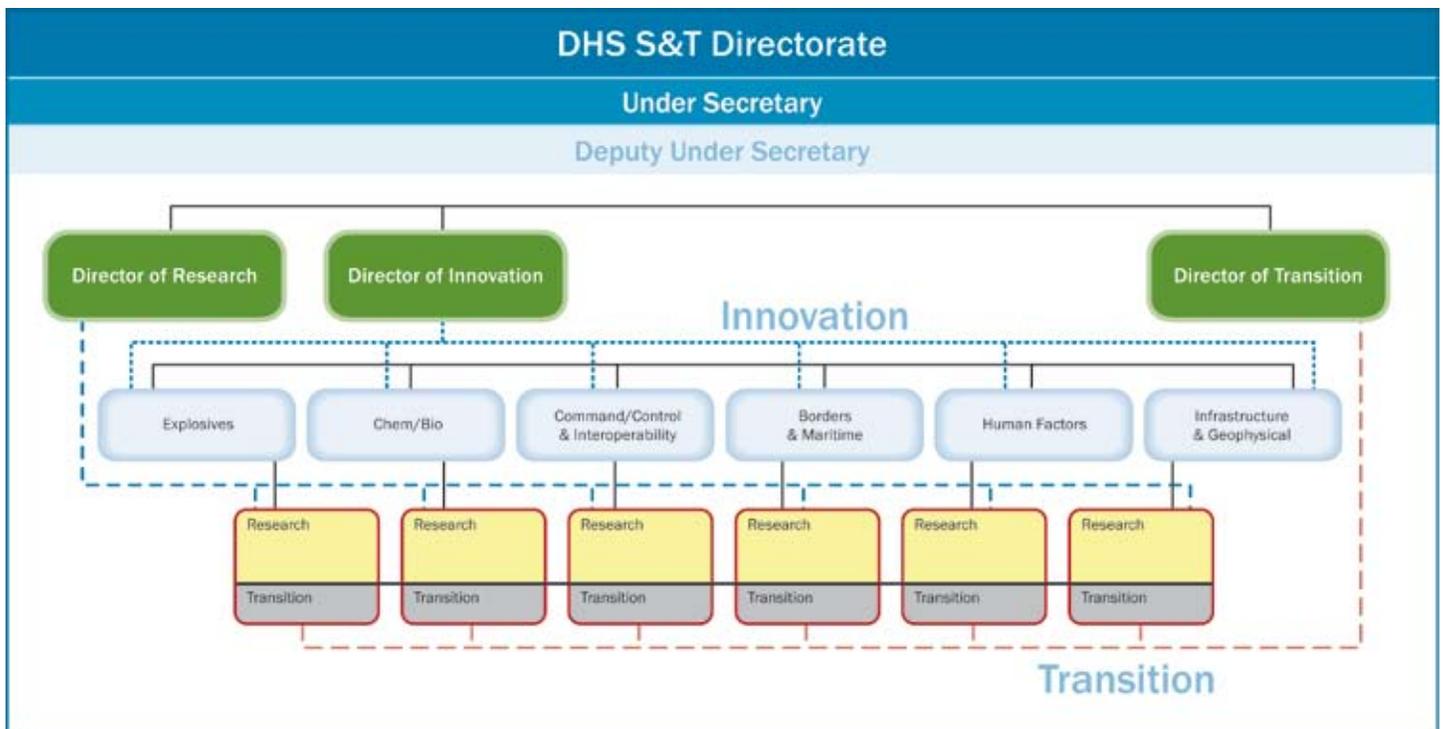
This appendix provides additional details on S&T programs and initiatives supporting the NIPP and CIKR protection. It includes details on how S&T is organized to produce and execute its investment strategy and how that strategy results in developing technology-based solutions to meet customer/end-user requirements.

6.1 S&T Organization and Investment Process

The organization of S&T results in an improved process to identify, validate, and procure new technologies, as well as to develop and integrate technology with the strategies, policies, and procedures required to protect the Nation's CIKR. The division's research, development, test, and evaluation (RDT&E) program achieves S&T strategic goals in six fundamental disciplines: (1) Explosives; (2) Chemical and Biological; (3) Command, Control, and Interoperability; (4) Borders and Maritime Security; (5) Human Factors; and (6) Infrastructure and Geophysical, which also represent S&T's six technical divisions.

These technical divisions are linked to three R&D investment portfolio directors in a "matrix management" structure. These three portfolio directors—the Director of Research, the Director of Transition, and the Director of Innovation/Homeland Security Advanced Research Projects Agency (HSARPA)—provide cross-cutting coordination of their respective elements (or thrusts) of the investment strategy within the technical divisions. Each technical division comprises at least one Section Director of Research who reports to the Director of Research (in addition to the Division Director) so that a cross-cutting focus on basic and applied research capabilities is maintained and leveraged. It also comprises a Section Director of Transition who reports to the Director of Transition (in addition to the Division Director) to help the division stay focused on technology transition.

The Director of Transition coordinates within the department to expedite technology transition and transfer to customers. The Director of Innovation/HSARPA sponsors basic and applied homeland security research to: promote revolutionary changes in technologies; advance the development, testing and evaluation, and deployment of critical homeland security technologies; and accelerate the prototyping and deployment of technologies that would address homeland security vulnerabilities and works



with each of the Division Heads to pursue game-changing, leap-ahead technologies that will significantly lower costs and markedly improve operational capabilities through technology application.

This cross-cutting coordination facilitates a unity of effort. The matrix structure also allows S&T to provide more comprehensive and integrated technology solutions to its customers by appropriately bringing all of the disciplines together in developing solutions.

6.1.1 R&D Investments and Planning

Along with the organizational alignment discussed above, S&T has also aligned its investment portfolio to create an array of programs that balance project risk, cost, mission impact, and the time it takes to deliver solutions. S&T executes projects across the spectrum of technical maturity and transitions them in accordance with customer needs. Its investment portfolio is balanced across long-term research, product applications, and leap-ahead, game-changing capabilities while also meeting mandated requirements. This balanced portfolio ensures that S&T maintains a self-replenishing pipeline of future capabilities and products to transition to customers.

The DHS Transition Program is a formalized, structured process that aligns investments with end-user requirements and is managed by Capstone Integrated Product Teams (IPTs). These teams constitute the Transition portfolio of S&T, targeting deployable capabilities in the near term. S&T established these teams to coordinate the planning and execution of R&D programs together with the eventual hand-off to the maintainers and users of the project results. They are critical nodes in the process for determining operational requirements, assessing current capabilities to meet operational needs, analyzing gaps in capabilities, and articulating programs and projects to fill in the gaps and expand competencies.

IPTs generally include the research and technology perspective, the customer/end-user perspective, and an acquisitions perspective. IPTs are specifically chartered to ensure that technologies are engineered and integrated into systems scheduled for delivery and made available to DHS customers and other homeland security partners. The customers/end-users monitor and guide the capability being developed; the research and technology representatives inform the discussions with scientific and engineering advances and emerging technologies; and the acquisitions staff help transition the results into practice by the maintainers and end-users of the capability.

The IPT topic areas reflect the capability requirements of homeland security stakeholders. The current IPTs operated by S&T are listed below. Each sponsors projects that are relevant to the CIKR protection mission. The three bolded IPTs are chaired or co-chaired by IP.

Information Sharing/Management	Counter IED
Border Security	Cargo Security
Chem/Bio Defense	People Screening
Maritime Security	Infrastructure Protection
Cyber Security	Preparedness & Response: Incident Management
Transportation Security	Preparedness & Response: Interoperability

Each IPT identifies, validates, and prioritizes requirements for S&T and provides critical input to investments in programs and projects that will ultimately deliver technology solutions that can be developed, matured, and delivered to customer acquisitions programs for deployment in the field. Investments are competitively selected and focus on DHS’s highest-priority, risk-based requirements that provide capabilities to customers/end-users. A successful transition portfolio requires sustained customer feedback from DHS components to ensure that programs address genuine capability gaps. To gain this insight, S&T established 46 Project IPTs and semi-annually reaches out to DHS components to gauge their overall satisfaction with delivered products and capabilities. The results are explicitly tied to the outcome-based performance metrics of cost, schedule, and technology readiness.

6.2 Requirements

S&T’s programs are motivated by the requirements of the DHS operating components and other homeland security partners. For CIKR protection, requirements are developed by the SSAs and their private sector and government partners. The National Risk Profile drives sector requirements, as well as the cross-sector prioritization of requirements. Prioritized requirements are, in turn, the basis for the NCIP R&D Plan, which advises investments across the Federal R&D community.

CIKR protection requirements have led to several initiatives and actions necessary for NIPP implementation, particularly regarding initiatives to:

- Review and revise CIKR-related plans, as needed, to reinforce the linkage between NIPP steady-state CIKR protection and NRF incident management requirements;
- Identify cross-sector vulnerabilities; and
- Communicate requirements for CIKR-related R&D to DHS for use in the national R&D planning effort.

6.2.1 High-Priority Technology Needs

Each year, S&T publishes the high-priority technology needs in its specified functional areas. The following is a representative sample of needs for the Nation’s CIKR:

- Analytical tools to quantify interdependencies and cascading consequences as disruptions occur across critical infrastructure sectors;
- Effective and affordable blast analysis and protection for critical infrastructure and an improved understanding of blast-failure mechanisms and protection measures for the most vital CIKR;
- Advanced, automated, and affordable monitoring and surveillance technologies, specifically, decision support systems to prevent disruption, mitigate results, and build resiliency;

- Rapid mitigation and recovery technologies to quickly reduce the effects of natural and manmade disruptions and cascading effects; and
- Critical utility components that are affordable and highly transportable, and provide robust solutions during manmade and natural disruptions.

6.2.2 Industry Involvement

Industry is a valued partner of S&T. Its continued participation in developing solutions for homeland security applications is vital to our effort to safeguard the Nation. Consistent with the directorate's new structure, the Innovation/HSARPA portfolio and six technical divisions will proactively seek industry participation to address specific challenges in their respective areas. Additionally, private sector owners and operators, through the SCCs, have provided powerful independent validation of the R&D priorities set by the Federal CIKR community. Several GCCs and SCCs have established joint R&D working groups to provide course-correcting input for future R&D direction.

6.3 Executing R&D Programs

Critical infrastructure is a widely distributed enterprise across multiple industries, government agencies, and academia, so its R&D program cannot be managed through a command and control-type process. Instead, DHS and OSTP are fostering an evolving network of partnerships and coordination groups. These groups have different focuses, including sector-specific needs, technology themes of interest to multiple sectors, and committees that coordinate Federal agency resources. The requirements process, translated into investment priorities, provides the goals and plans that allow this distributed R&D enterprise to act in coordinated ways. The National Annual Report and the NCIP R&D Plan communicate this overarching R&D strategy and help identify which R&D requirements are best met by the private versus the public sector.

6.3.1 Partnerships and Collaboration

The NIPP Partnership Framework

The CIPAC, established by DHS, has been very effective in helping Federal infrastructure protection groups work with the private sector and with State, local, tribal, and territorial governments. The CIPAC provides a forum in which the sectors have engaged very actively in a broad spectrum of activities to implement their sector protection plans, including planning, prioritizing, and coordinating R&D agendas.

Sector and Cross-Sector Coordination

The Sector R&D Working Groups, typically Joint SCC and GCC, have developed well-founded technical R&D agendas that are essential for their sector in order to achieve sector security goals. These R&D agendas coordinate challenges across the spectrum of sector stakeholders and are used to represent sector R&D interests in cross-sector settings. The executive managers of each sector coordinate activities through the FSLC. The SCCs have formed a cross-sector group, the CIKR Cross-Sector Council,²⁸ to coordinate cross-sector initiatives that promote public and private infrastructure protection initiatives. One of the objectives of the CIKR Cross-Sector Council is to provide cross-sector input regarding R&D priorities; this input is informed by the results of risk assessments in each sector, as well as the National Risk Profile.

Universities

Universities and research centers across multiple Federal agencies contribute to agency mission accomplishment and CIKR protection from the time before a disruptive event to the time after a disruptive event. The DHS Centers of Excellence contribute to the national-level implementation of the NIPP and to CIKR protection; their contributions take different forms, including the following:

²⁸ The CIKR Cross-Sector Council comprises the leadership of each of the SCCs; the Partnership for Critical Infrastructure Security currently provides this representation.

- Provide independent analysis of CIKR protection (full-spectrum) issues;
- Conduct research and provide innovative perspectives on threats and the behavioral aspects of terrorism;
- Conduct research to identify new technologies and analytical methods that can be applied by CIKR partners to support NIPP efforts;
- Support research, development, testing, evaluation, and deployment of CIKR protection technologies;
- Analyze, provide, and share best practices related to CIKR protection efforts; and
- Develop and provide suitable security risk analysis and risk management courses for CIKR protection professionals.

International

DHS, DoD, DOE, and other Federal agencies have undertaken many different outreach efforts to foreign government representatives and organizations that are pursuing similar R&D planning and performance. Agreements of cooperation, joint pursuit, and knowledge sharing have been created with France, Germany, Japan, Israel, Italy, the Netherlands, Russia, the Scandinavian countries, the United Kingdom, and others. Other organizations, such as the TSWG, also have developed successful R&D collaborations with a number of countries.

State and Local

State, local, tribal, and territorial governments play an important role in the protection of the Nation's CIKR. These governmental entities not only have CIKR under their direct control, but also have CIKR owned and operated by other partners who are within their jurisdictions. The SLTTGCC and RCCC bring national CIKR protection principles to the State, local, and regional levels and are important sources of capability requirements that drive R&D priorities.

Industry Organizations

In addition to R&D input provided by government organizations, there are major industrial groups that provide input and comment in order to influence future R&D by illuminating issues that they have encountered and issues that are likely based on new product development that they are doing but cannot discuss openly for competitive reasons. For example, the INFOSEC Research Council has provided valuable input on cybersecurity, including the publication of a Hard Problems List²⁹ that is an important planning tool used by all R&D contributors. The NSTAC identified critical gaps that require new cyber and telecommunications R&D.

6.4 Five-Year Strategy/Technology Roadmap

S&T implements its business approach through its Planning, Programming, Budgeting, and Execution (PPBE) process, which encompasses the development of priorities, program plans, resource requirements, and associated performance metrics. The PPBE process builds the framework to link strategy for the out-years to program execution in the present. It ensures that the directorate remains mission-focused, customer-oriented, and threat- and risk-informed in order to prioritize resource allocation and remain accountable in its efforts to secure the homeland.

The 5-year execution plan: details the S&T investment portfolio; outlines the directorate's activities and plans at the division level; and includes each division's research thrusts, programs, and key milestones. It supports the department's strategic plan and priorities, as well as S&T's priorities. The 5-year plan is the roadmap for achieving success; however, the planning process must be flexible in order to adjust to a changing homeland security environment. The plan will be updated annually to ensure that it continues to address the correct set of priorities, fills customers' homeland security capability gaps, and enables the achievement of a safer homeland.

²⁹ See http://www.cyber.st.dhs.gov/docs/IRC_Hard_Problem_List.pdf.







Homeland
Security

Appendix B: ORD Examples

Learn by Doing:

**Developing a detailed Operational Requirements Document
(ORD)**

Requirements Development Initiative – Operational Requirements Document (ORD) Examples

This compilation of ORDs is meant to present the reader with several real-world examples of detailed operational requirements drafted by implementing an easy-to-use ORD template that provides a basic framework in guiding the articulation and communication of needs.

Please keep in mind the following points as you consider writing an ORD to describe and define an existing problem:

1. Writing an ORD is **not** as difficult as you think → so just “jump in” and give it a try
2. We’re here to help! Please use the many resources available online at http://www.dhs.gov/xres/programs/gc_1211996620526.shtm and <https://dhsonline.dhs.gov/portal/jhtml/community.jhtml?index=15&community=S%26T&id=2041380003> for guidance:
 - ORD templates
 - Example ORDs
 - “Developing Operational Requirements” (Version 2)
3. Some simple things to remember:
 - **Requirements** define problems while **specifications** define solutions
 - An ORD describes a problem, not a solution
 - Make sure your ORD is product/service/solution agnostic (that is, it does **not** presuppose a certain solution)
 - Make the solution space as wide as possible
 - Keep it simple and make it easy for a reader to understand your problem/requirement
4. Review the attached ORD template examples and contact us if you have any questions or comments!
 - SandT.Commercialization@hq.dhs.gov

ORD Template and Examples

OPERATIONAL REQUIREMENTS DOCUMENT Template	241
Portable Stand Alone Water Purification	246
Blast Resistant Autonomous Video Equipment (BRAVE)	254
Predictive Modeling for Counter-Improvised Explosive Devices	263

OPERATIONAL REQUIREMENTS DOCUMENT

[Name of System or Product]

to be developed by the
[Name of Acquisition Program]

[Name of Program Manager]
Program Manager, [Name of Acquisition Program]
[Name of PM's Organization]

[Name of Sponsor]
Sponsor, [Name of Acquisition Program]
[Name of Sponsor's Organization]

[Name of S&T Project Manager]
Project Manager, [Name of S&T Project]
[Name of S&T Division]
Science and Technology Directorate

Date
Version X.X

Contents

1. General Description of Operational Capability	243
1.1 Capability Gap.....	243
1.2 Overall Mission Area Description.....	243
1.3 Description of the Proposed Product or System	243
1.4 Supporting Analysis	243
1.5 Mission the Proposed System Will Accomplish.....	243
1.6 Operational and Support Concept	243
1.6.1 Concept of Operations.....	243
1.6.2 Support Concept.....	243
2 Threat	243
3 Existing System Shortfalls	243
4 Capabilities Required	244
4.1 Operational Performance Parameters	244
4.2 Key Performance Parameters (KPPs)	244
4.3 System Performance.	244
4.3.1 Mission Scenarios.....	244
4.3.2 System Performance Parameters.....	244
4.3.3 Interoperability.....	244
4.3.4 Human Interface Requirements	244
4.3.5 Logistics and Readiness.....	244
4.3.6 Other System Characteristics.....	244
5 System Support.....	244
5.1 Maintenance.....	244
5.2 Supply	245
5.3 Support Equipment	245
5.4 Training	245
5.5 Transportation and Facilities.....	245
6 Force Structure.....	245
7 Schedule.....	245
8 System Affordability	245

1.

1. General Description of Operational Capability

In this section, summarize the capability gap which the product or system⁹ is intended to address, describe the overall mission area, describe the proposed system solution, and provide a summary of any supporting analyses. Additionally, briefly describe the operational and support concepts.

1.1. Capability Gap

Describe the analysis and rationale for acquiring a new product or system, and identify the DHS Component which contains or represents the end users. Also name the Capstone IPT, if any, which identified the capability gap.

1.2. Overall Mission Area Description

Define and describe the overall mission area to which the capability gap pertains, including its users and its scope

1.3. Description of the Proposed Product or System

Describe the proposed product or system. Describe how the product or system will provide the capabilities and functional improvements needed to address the capability gap. Do not describe a specific technology or system solution. Instead, describe a conceptual solution for illustrative purposes.

1.4. Supporting Analysis

Describe the analysis that supports the proposed system. If a formal study was performed, identify the study and briefly provide a summary of results.

1.5. Mission the Proposed System Will Accomplish

Define the missions that the proposed system will be tasked to accomplish.

1.6. Operational and Support Concept

1.6.1. Concept of Operations

Briefly describe the concept of operations for the system. How will the system be used, and what is its organizational setting? It's appropriate to include a graphic which depicts the system and its operation. Also describe the system's interoperability requirements with other systems.

1.6.2. Support Concept

Briefly describe the support concept for the system. How will the system (hardware and software) be maintained? Who will maintain it? How, where, and by whom will spare parts be provisioned? How, where, and by whom will operators be trained?

2. Threat

If the system is intended as a countermeasure to a threat, summarize the threat to be countered and the projected threat environment.

3. Existing System Shortfalls

Describe why existing systems cannot meet current or projected requirements. Describe what new capabilities are needed to address the gap between current capabilities and required capabilities.

⁹ In this document, the terms "product" and "system" are synonymous. The word "system" is used to refer to either.

4. Capabilities Required

4.1 Operational Performance Parameters

Identify operational performance parameters (capabilities and characteristics) required for the proposed system. Articulate the requirements in output-oriented and measurable terms. Use Threshold/Objective¹⁰ format and provide criteria and rationale for each requirement.

4.2 Key Performance Parameters (KPPs)

The KPPs are those attributes or characteristics of a system which are considered critical or essential. Failure to meet a KPP threshold value could be the basis to reject a system solution.

4.3 System Performance.

4.3.1 Mission Scenarios

Describe mission scenarios in terms of mission profiles, employment tactics, and environmental conditions.

4.3.2 System Performance Parameters

Identify system performance parameters. Identify KPPs by placing an asterisk in front of the parameter description.

4.3.3 Interoperability

Identify all requirements for the system to provide data, information, materiel, and services to and accept the same from other systems, and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together.

4.3.4 Human Interface Requirements

Discuss broad cognitive, physical, and sensory requirements for the operators, maintainers, or support personnel that contribute to, or constrain, total system performance. Provide broad staffing constraints for operators, maintainers, and support personnel.

4.3.5 Logistics and Readiness

Describe the requirements for the system to be supportable and available for operations. Provide performance parameters for availability, reliability, system maintainability, and software maintainability.

4.3.6 Other System Characteristics

Characteristics that tend to be design, cost, and risk drivers.

5. System Support

Establish support objectives for initial and full operational capability. Discuss interfacing systems, transportation and facilities, and standardization and interoperability. Describe the support approach including configuration management, repair, scheduled maintenance, support operations, software support, and user support (such as training and help desk).

5.1 Maintenance

Identify the types of maintenance to be performed and who will perform the maintenance. Describe methods for upgrades and technology insertions. Also address post-development software support requirements.

¹⁰ The threshold value for a requirement is the minimum acceptable performance. The objective value is the desired performance.

5.2 Supply

Describe the approach to supplying field operators and maintenance technicians with necessary tools, spares, diagnostic equipment, and manuals.

5.3 Support Equipment

Define the standard support equipment to be used by the system. Discuss any need for special test equipment or software development environment

5.4 Training

Describe how the training will ensure that users are certified as capable of operating and using the proposed system.

5.5 Transportation and Facilities

Describe how the system will be transported to the field, identifying any lift constraints. Identify facilities needed for staging and training.

6. Force Structure

Estimate the number of systems or subsystems needed, including spares and training units. Identify organizations and units that will employ the systems being developed and procured, estimating the number of users in each organization or unit.

7. Schedule

To the degree that schedule is a requirement, define target dates for system availability. If a distinction is made between Initial Capability and Full Operational Capability, clarify the difference between the two in terms of system capability and/or numbers of fielded systems.

8. System Affordability

Identify a threshold/objective target price to the user at full-rate production. If price is a KPP, include it in the section on KPPs above.

Operational Requirements Document: Portable Stand Alone Water Purification Contents

1. General Description of Operational Capability	247
<i>1.1. Capability Gap</i>	247
<i>1.2. Overall Mission Area Description</i>	247
<i>1.3. Description of the Proposed Product or System</i>	248
<i>1.4. Supporting Analysis</i>	248
<i>1.5. Mission the Proposed System Will Accomplish</i>	248
<i>1.6. Operational and Support Concept</i>	248
1.6.1. Concept of Operations	248
1.6.2. Support Concept	249
2. Threat	249
3. Existing System Shortfalls	250
4. Capabilities Required	251
<i>4.1. Operational Performance Parameters (T: Threshold/ O: Objective)</i>	251
<i>4.2. Key Performance Parameters (KPPs)</i>	251
<i>4.3 System Performance.</i>	251
4.3.1 Mission Scenarios	251
4.3.2 System Performance Parameters	251
4.3.3 Interoperability	252
4.3.4 Human Interface Requirements.....	252
4.3.5 Logistics and Readiness	252
4.3.6 Other System Characteristics	252
5. System Support	252
<i>5.1 Maintenance</i>	252
<i>5.2 Supply</i>	253
<i>5.3 Support Equipment</i>	253
<i>5.4 Training</i>	253

Example Only

5.5 Transportation and Facilities.....253
6. Force Structure.....253
7. Schedule.....253
8. System Affordability253

1. General Description of Operational Capability

Water is a basic necessity for human life. In the event of a natural disaster or terrorist attack, the ability to quickly deliver potable water to communities is of critical importance.

With a cost-effective and ergonomic purification system on-site, government agencies, emergency management professionals and first responder teams can curb the all-too-often costly and polluting practice of trucking water into affected areas, not to mention eliminating or greatly reducing the burden of having to dispose of many thousands of discarded water bottles and other trash.

The operational capability described in this operational requirements document (ORD) will provide users with a self-contained, self-fueling water pumping and purification system that can be deployed and operated in less than thirty minutes after transport to a site by truck, helicopter or boat. Units shall be operated without specialized training wherever the need for potable water or water displacement arises. A proposed system shall provide an affordable, high-quality, easy-to-use option utilizing reliable technology at significant cost savings over the current methods providing potable water to users in need.

1.1. Capability Gap

The conventional method of providing potable water in the wake of a disaster is often costly and logistically complex. Normally, potable water is distributed to communities by trucking in bottled water or using diesel generator purification systems.

Any proposed system must eliminate many points of failure by presenting a stand-alone design allowing for flexible transport of the unit by air, land or water bringing a cost-effective, high-yield water purification capability to potential users incorporating a self-generating power source.

1.2. Overall Mission Area Description

The provision of potable water to communities affected either by natural disasters or terrorist events is understandably a top priority for first responders, emergency management authorities at all levels of government concerned with short and medium term disaster response and relief efforts.

Any proposed system shall provide a stand-alone potable water resource to federal, state, local and tribal preparedness and/or response teams and emergency management professionals. A proposed system shall be transportable using a variety of options (by air, land and/or water) even in the most adverse conditions. A proposed system shall be easy-to-deploy, easy-to-use, and shall produce potable water from even polluted sources.

Example Only

Any proposed system shall be low cost, low maintenance, providing high quality and high yield output. A system shall primarily be used to pump and purify water for public consumption with ancillary benefits such as self-generating power to operate its pumps as well as provide DC and AC load centers into which other critical equipment could be plugged in and engaged. This is especially required in areas that have been devastated by a natural disaster or terrorist event where infrastructure, electrical, transportation and water resources have been compromised.

1.3. Description of the Proposed Product or System

A proposed system shall be a self-contained, self powered water purification system contained in as small as possible foot-print. The system shall be deployed to any site where there is level ground using forklift, helicopter, truck or boat and shall easily fit into any shipping container. No special training shall be required to operate a proposed system, and a system shall be operable, pumping and purifying water and supplying electricity in less than 30 minutes after arrival on site. A proposed system shall eliminate particles and render biological pathogens inert. A multi-thousand gallon collapsible storage tank shall come standard with each unit, storing water so it is available when needed by first responders and community members. A proposed system shall contain an internal battery bank (or equivalent) so that the system can operate 24/7 and can also provide electricity to run generators, lights, tools or other command station equipment.

1.4. Supporting Analysis

Countless requests from members of the first responder community know that such kinds of systems have been used effectively in other applications in other venues.

1.5. Mission the Proposed System Will Accomplish

Any proposed system shall provide readily-deployable, high quality, high yield water purification to disaster-affected communities at a low cost. Any proposed system shall eliminate any and all problems associated with bottled water or more cumbersome fuel alternatives often used to provide potable water. The proposed system shall be easily deployable and operational in a self-contained, self-generating powered platform eliminating the need to supply additional fuel. With the capability of 24/7 operation, potable water needs to be readily available at a site, when and where it is most needed, at a low cost with no pollution. Ancillary power available to operate lights, computers, satellite communications modules and other equipment is also required.

1.6. Operational and Support Concept

1.6.1. Concept of Operations

A proposed system may be deployed after a disaster event to affected areas to purify contaminated water sources or may be transported to a site where it is likely to be needed before the occurrence of a natural event. For instance, if it is likely a hurricane will make landfall in a particular area, a proposed system shall possess the ability to be pre-positioned. A proposed system shall be able to withstand commonly occurring weather conditions without additional hardening or protection. A system safety plan shall be provided for necessary precautions to protect a proposed system from weather disasters such as tornados, hurricanes, etc.

Emergency response teams making use of the system shall identify areas requiring water purification based on local procedures, emergency response plans and readiness of a

Example Only

water source, including identification of specific deployment locations. Water test kits shall be provided with each unit, and additional kits shall be made available at a low price from the vendor to test pre- and post-filtration water quality.

Operation roles in the field will be determined by local procedures and emergency response plans. A comprehensive, easy-to-understand training manual shall be included with each unit describing the procedures to deploy and operate a system. In the event a more in-depth training session is required, a provider shall host tailored training sessions. A system provider shall provide telephone, email and on-site assistance plans, as necessary.

Any proposed system shall be capable of utilizing other power sources such as grid or generator, when available, as a “back up” to its self-generating power. Power generated by the unit is used to pump and purify water and can also be used to power ancillary tools, lights and communication systems.

A system shall be self-contained and self-powered.

1.6.2. Support Concept

Any system shall support easy installation and maintenance without the general need for specialized training. Maintenance requirements shall be minimal.

Maintenance and operation roles in the field will be conducted by personnel using local procedures and emergency response plans. A comprehensive operations manual shall be provided with each unit describing when routine maintenance is required and the procedures required to maintain a given system. In the event a more in-depth training session is requested, the vendor hosts regular training sessions. Any supplier shall provide on-site assistance plans as well as telephone and email troubleshooting assistance.

Any system consumables shall be available for up to seven years after original system purchase.

2. Threat

Contaminated water poses a significant health risk to exposed individuals. Exposure to contaminated water can result in sickness and death.

Water infrastructure represents a potential terrorist target. Having in place a system ready to deploy to an affected area a high yield ($\geq 30,000$ gallons from freshwater sources) of purified water is critical to necessary preparation for providing potable water to communities.

Additionally, water sources are often contaminated during a natural disaster. Hurricane events along the U.S. Gulf Coast, including Hurricane Katrina (2005) and Hurricane Gustav (2008) regularly impact water resources adversely, leaving communities without access to sanitary water. Other natural disasters have caused similar devastation to communities by contaminating water supplies including the 2004 Indian Ocean Tsunami and the earthquake in Sichuan, China (2008).

3. Existing System Shortfalls

The current methods of providing potable water in the wake of a disaster can be both costly and logistically complex. Current methods of distributing potable water to communities is trucking in bottled water or using diesel generator purification systems. The shortfalls in these approaches can include the high cost and logistical considerations of buying and transporting fuel and buying and transporting bottled water, as well as disposal costs of used bottles. These traditional approaches require roads and bridges to be passable in order to transport the goods, and also require ongoing monetary outlay to purchase fuel, transport the goods and personnel to oversee and fuel generators. A proposed system shall utilize technology to significantly reduce logistical considerations inherent in the provision of potable water where clean water is unavailable and also offer significant cost savings.

For example, hurricane, tornado, earthquake and other disaster response plans have typically provided bottled water to affected communities with potential ongoing difficulties, including:

- sourcing water vendors.
- costly contracts to purchase bottled water and transportation services.
- fluctuating cost of fuel, making budget planning difficult.
- diluted distribution system which can be difficult to oversee and ensure quality of service delivery.
- unreliable roads and other infrastructure needed to deliver the bottled water.
- unreliable delivery dates presenting the possibility of no potable water to distribute.
- costly disposal of discarded water bottles and the resulting increase of waste diverted to landfills and/or costs associated with the recycling of discarded bottles.

Diesel-only generator purification systems can present similar difficulties in terms of high cost, the necessity of having a readily available and cheap source of fuel and an easy, cost effective means of regularly transporting the fuel to an affected site.

In summary, conventional methods of delivering potable water after a disaster rely on three uncontrollable factors:

- (1) the identification and ability of a source to supply bottled water or generator fuel,
- (2) the availability of fuel to transport goods,
- (3) an intact transportation infrastructure network to get the goods to an affected site.

These three points of potential failure in more typical approaches are present throughout the duration of a disaster response. Any proposed system shall eliminate these potential points of failure by presenting a stand-alone design allowing for flexible transport of the unit by air, land and/or water bringing high-yield water purification to an affected site and using self-generating power capabilities thus eliminating the need for only external fuel sources for operation.

Current methods present a threat of interrupted service when any one of these factors fails at anytime during the short and medium term of disaster response, leaving communities without life-saving water for undefined periods of time. Current methods rely on functional transportation networks to move bottled water or diesel generator fuel to the site. The transport of these goods can be costly as is often the purchase of goods (i.e. the bottled waters). Costs associated with the disposal of bottled water containers is another potential shortcoming of this type of approach.

Capabilities needed to address this gap include utilization of a stand-alone water purification system on-site that does not require external fuel sources alone. It is also important that the technology be initially transportable to the site using a variety of transportation methods in order

Example Only

to mitigate impassable roads and bridges. This ensures that potable water is being delivered to affected communities without interruption of service.

4. Capabilities Required

4.1. Operational Performance Parameters (T: Threshold/ O: Objective)

- Each system unit will weigh no more than 8,000 pounds (T) and \leq 5,000 pounds (O).
- Stowed, the units are no more than 10x10x10 foot cube (T), 5x5x5 foot cube (O).
- Each unit will have a total capacity of \geq 3000 watts (T), \geq 4,000 watts (O) when fully operational.
- Grid power connection to allow for trickle charging during long-term indoor storage (T)/ (O).
- Ability to run additional equipment from 120VAC and 12 VDC plugs (T), 120VAC or 220VAC and 12 VDC plugs (O).
- A system shall pump and purify an average of \geq 20 gallons per minute (GPM) (T), \geq 30 gallons per minute (O) from freshwater surface or shallow well sources when fully operational. Capabilities to purify saltwater and brackish water sources shall also be available.

4.2. Key Performance Parameters (KPPs)

- Easily transportable to the site using truck (and trailer,) international shipping container, boat, helicopter and/or forklift (T)/ (O).
- Easy to use with limited training (T), after review of operation manual (O).
- Each unit is self-powered (T)/ (O).
- A system shall pump and purify an average of \geq 20 gallons per minute (GPM) (T), \geq 30 gallons per minute (O) from freshwater surface or shallow well sources when fully operational. Capabilities to purify saltwater and brackish water sources shall also be available.
- Filtration process without using chemicals to purify water (T), providing redundancy for safety and uninterrupted water purification output, without using chemicals to purify water (O).
- Water filtered by a system must meet the standards for Drinking Water Quality set forth by the Environmental Protection Agency (EPA), and provisions of the Safe Drinking Water Act of 1974 and all subsequent amendments (T)/ (O).

4.3 System Performance.

4.3.1 Mission Scenarios

Any proposed system shall work in defined harsh environments and represent a tool for emergency management professionals and disaster relief teams. Any proposed system shall be self-contained, easily transportable and easy-to-use system that purifies contaminated water at the source, at a low cost while providing the added benefits of being self powered, and providing ancillary power to operate additional AC and DC machinery.

4.3.2 System Performance Parameters

- Each unit is self-powered (T)/ (O).

Example Only

- The system can pump and purify an average of ≥ 20 gallons per minute (GPM) (T), ≥ 30 gallons per minute (O) from freshwater surface or shallow well sources when fully operational. There are also capabilities to purify seawater and brackish water sources.
- Filtration process shall occur without using chemicals to purify water (T), providing redundancy for safety and uninterrupted water purification output, without using chemicals to purify water (O).

4.3.3 Interoperability

Any proposed system shall work independently, without relying solely on any external input. It generates its own electricity to power water pumps, water purification and other equipment. In order to provide the utmost flexibility to the end user, the system can also be tied in seamlessly to the grid (and use other forms of energy in “back-up” modes)

4.3.4 Human Interface Requirements

Operator safety is paramount. Safety features shall be incorporated into the unit. A system shall be deployed by no more than two people in ≤ 30 minutes using the easy-to-follow operation manual.

Any proposed system shall require minimal maintenance and oversight, while including safety mechanisms to ensure high quality of potable water output. It only requires periodic visual confirmation from an operator to ensure the system is running optimally, checking system indicators and flow of potable water coming out of the purification system.

4.3.5 Logistics and Readiness

Safety features shall be built into a system to ensure the highest quality water output.

Operators shall be easily alerted if any filters or other consumables must be changed or serviced.

4.3.6 Other System Characteristics

Any proposed system shall operate in harsh environments and operate in temperatures ranging from at least 32-degrees to above 120-degrees (F), high humidity, rainfall, high wind and dust-filled environments. Any system or unit shall have at least a 5-year guarantee of performance under stated, normal conditions.

5. System Support

5.1 Maintenance

Any proposed system shall be designed to require minimal maintenance and oversight, while including safety mechanisms to ensure high quality of potable water output. Periodic visual checks of a system’s self diagnostic indicators will be conducted by operators or maintenance personnel to ensure the system is running optimally, checking potential gauges, LED light indicators and flow of potable water coming out of the purification system. Minimal training of personnel is required to ensure proper understanding of system self-diagnostic indicators.

An operation manual shall show the procedures required to maintain/change consumables and accomplish routine maintenance.

Example Only

5.2 Supply

Operation and maintenance manual(s) shall be provided to an end user with each system. Manuals will include deployment procedures, information on diagnostics, a troubleshooting guide and consumable replacement procedures. Any supplier shall provide low-cost replacement packages for standard water purification consumables.

5.3 Support Equipment

No additional equipment shall be required for the operation of a system.

5.4 Training

A training manual shall be provided with each system describing when routine maintenance should be performed and procedures required to maintain a system. In the event a more in-depth training session is required, a supplier shall host customizable training session(s). On-site assistance plans, as well as telephone and email troubleshooting assistance shall be provided.

5.5 Transportation and Facilities

Any system shall be transported by truck, trailer, air, in international shipping containers, by boat, by helicopter suspended from installed lift points or by forklift using the skids built into the base of each system. A system shall be installed at a minimum on level ground or on a trailer bed near a water source.

6. Force Structure

Emergency Response teams at the state, local and/or tribal level are the typical customers. Any proposed system shall not require specialized knowledge or training to operate or maintain.

It is conservatively estimated that the potential available market for such a system is greater than 18,000 units for use by local municipalities, public water systems, water treatment facilities and emergency management agencies, for example.

7. Schedule

Units or systems shall be available for purchase in 12 months or less after signing SECURE Program agreement. Deployment of the units typically shall require less than thirty minutes after arriving on site. Units can be deployed without any specialized training.

8. System Affordability

Individual system price is not expected to exceed \$100,000 at high volume production levels (T), ≤ \$80,000 for a freshwater system (O).

Systems for the purification of brackish and/or seawater sources shall also be available in less than 18 months. Replacement consumable parts can be readily purchased from a supplier for at least five years after purchase.

Systems shall also be available to potential users on a lease or lease-to-buy payment scheme.

Operational Requirements Document (ORD)

Blast Resistant Autonomous Video Equipment (BRAVE)

Contents

1. General Description of Operational Capability.....	255
1.1. Capability Gap	256
1.2. Overall Mission Area Description	256
1.3. Description of the Proposed System.....	256
1.4. Supporting Analysis.....	257
1.5. Mission the Proposed System Will Accomplish.....	257
1.6. Operational and Support Concept.	257
1.6.1. Concept of Operations	257
1.6.2. Support Concept	258
2. Threat	258
3. Existing System Shortfalls	258
4. Capabilities Required.....	259
4.1. Operational Performance Parameters (T: Threshold / O: Objective)	259
4.1.1. Form Factor	259
4.1.2. Resolution.....	259
4.1.3. Frame Rate.....	259
4.1.4. Field of View/Focal Length:	259
4.1.5. Data Format	259
4.1.6. Tamper Resistance	259
4.1.7. Power Source	259
4.1.8. Environmental	259
4.1.9 Blast Survivability.....	260
4.2. Key Performance Parameters (KPPs).....	260
4.2.1. Cost.....	260
4.2.2. Storage Capacity.....	260
4.3 System Performance.....	260
4.3.1 Mission Scenarios.....	260
4.3.2 Interoperability	261

Example Only

4.3.3 Human Interface Requirements 261

4.3.4 Logistics and Readiness 261

5. System Support.....261

5.1 Maintenance..... 261

5.2 Supply 261

5.3 Support Equipment 261

5.4 Training 262

5.5 Transportation and Facilities 262

6. Force Structure.....262

7. Schedule262

8. System Affordability.....262

1. General Description of Operational Capability

The rapid development of low cost forensic camera systems for use by the First Responder community and ancillary markets will give state, local and tribal and transit authorities the ability to determine incident cause at a low total cost of ownership in numerous applications. While technologies are currently being explored and developed at locales like Chicago, LA, Seattle and other metropolitan areas, a low cost alternative with high rapid potential deployment to more users compared to these more costly systems is attractive for many reasons.

In one example, mass transit vehicles and networks represent a potentially attractive target to terrorists and a unique challenge for law enforcement and transit personnel, due to their relative openness and large user base. Recent attacks in London, Madrid, and elsewhere around the world have demonstrated the devastating impacts of attacks carried out on mass transit vehicles. The investigation of the July 2005 attacks in London also demonstrated the forensic power of employing video surveillance data to successfully identify the terrorists directly and indirectly involved in such an attack.

While many communities and transit agencies in the United States have implemented the use of video surveillance systems within their transit infrastructure, uniformity of coverage is lacking. Financial, technical, and policy challenges continue to limit the implemented coverage. As a result, the requirement exists to enhance the capability to obtain, store and protect video surveillance information gathered from mass transit systems for forensic purposes.

The operational capability described herein, will provide user communities with a self-contained low-cost video surveillance option that can be implemented as an adjunct to an existing system or as a primary source for forensic video surveillance information. The system will support greater surveillance implementation and meet a range of surveillance requirements for operators in applications where infrastructure intensive approaches are impractical.

Example Only

1.1. Capability Gap

A gap currently exists in the surveillance coverage of national critical infrastructure. For example, the majority of major mass transit systems are not able to reliably collect, store and protect video surveillance of potential future terrorist attacks throughout their transit networks. While specific technical capabilities exist, coverage is limited in many localities due to high costs and infrastructure requirements of existing systems. Except in select localities (e.g. Chicago), most cities have video surveillance capabilities in a small percentage of mass transit buses and often less in rail applications. This coverage gap directly limits the ability to investigate, pursue, and prosecute terrorists following a potential terrorist act involving non-covered conveyances.

Infrastructure intensive technical approaches present a capability gap for mobile platforms (e.g. buses and trains) where sufficient transmission bandwidth may not be available, is cost prohibitive, and may raise security concerns. Existing surveillance approaches typically require an extensive wired (or wireless) network to support high bandwidth transmission of data to centralized processing and storage facilities. Centralized networked systems also incur intensive manpower requirements for installation, monitoring, and maintenance.

Pursuit of the system described herein will facilitate the closing of the coverage gap in video surveillance coverage by providing a low cost capability to supplement existing capabilities and coverage or a stand-alone system in the case where no legacy capability exists. The intended end users of the system are the impacted local transit authorities (represented within DHS by Transportation Security Administration – Rail and Surface Transportation), transit and local law enforcement officers, and the federal agencies involved in the forensic investigation of a terrorist attack.

1.2. Overall Mission Area Description

Video surveillance systems are currently used by mass transit operators and associated law enforcement departments for a wide range of missions. Mission applications include support of transit operations, criminal investigation, litigation support, enforcement of passenger regulations, training, and improved safety of passengers and employees due to a deterrent effect.

The system identified herein will have the additional capability to protect recorded video surveillance data, without external infrastructure, in the event of a terrorist attack, and to support forensic investigation of the same. The system is expected to provide coverage of areas not currently reached by video surveillance and in some cases to provide supplementary blast resistant video coverage in areas currently service by other systems. In addition to post terrorist attack forensics, the system is expected to extend coverage of other mission applications including criminal investigation and litigation support to newly covered areas. Due to its decentralized approach, however, the system will not directly support mission applications requiring real time monitoring of data (e.g. support to transit operations).

1.3. Description of the Proposed System

The proposed system will be a stand-alone fixed video surveillance unit that will produce and maintain a continuous video recording of a designated transit vehicle, infrastructure component, access control point, or other location of interest within its designated field of

Example Only

view. It is expected that multiple such units will be necessary to provide full coverage of individual transit vehicles and other areas of interest. Each unit will record continuously and store data for a specified period of time, after which data will automatically be overwritten as necessary. Following installation, the system will not require user intervention to maintain continued operation.

In the event of a terrorist attack or catastrophic event, the unit will protect the recorded data from damage or tampering until retrieval by authorities. Only survival of the video data sufficient for retrieval and playback of the collected video surveillance is expected. The system will also allow for data retrieval by authorized individuals as required for other mission applications.

Each BRAVE unit will be a self contained device that includes a camera, removable data storage, and protective hardening for the data storage. System power may be provided by the installed platform (e.g. bus) or by an included power source. In the case of an external power option, a transformer, as necessary, will be included within the system housing.

1.4. Supporting Analysis

This ORD is supported by “Application of Video Surveillance Technology in Public Transit Systems” submitted to DHS S&T through the U.S. Army Natick Soldier Research Development and Engineering Center (NSRDEC) and prepared by the Center for Technology Commercialization. The analysis is further supported by visits to transit authorities in Seattle, WA; Washington, DC; New York, NY; and Chicago, IL conducted by NSRDEC and DHS S&T representatives in February 2008.

1.5. Mission the Proposed System Will Accomplish

The proposed system will provide a low-cost option for provision of a blast-resistant video surveillance capability to mass transit platforms without such a capability. Once installed, BRAVE will support investigation of terrorist and criminal activities conducted within the visual coverage of the deployed system.

The system will serve primarily to visually record all activity within its field of view for a designated period of time. Video data will be recorded continuously during designated operational periods. Video data stored beyond the designated storage duration will be overwritten as necessary to provide storage for more recent video data. In the event of an explosion caused by a terrorist attack, the system will protect the data from blast and other damage and allow recovery of the video data for purposes of forensic investigation and/or prosecution.

1.6. Operational and Support Concept

1.6.1. Concept of Operations

BRAVE will be used by local transit authorities and law enforcement officials to supplement video surveillance coverage in areas and vehicles not currently covered by legacy systems. Localities making use of the system will identify areas requiring coverage based upon their local procedures, including identification of specific installation locations.

Example Only

Transit maintenance or contracted personnel will install units in identified locations including connection to locally available power source as applicable. Upon installation, each unit will provide continuous video recording whenever powered. User support and maintenance will be minimal.

Retrieval of data will use commercially standard interfaces (e.g. Secure Digital card, or USB connection) to retrieve data. Video will similarly be stored in a commercially standard, non-proprietary format to facilitate easy review of data in a range of commercially available software applications.

1.6.2. Support Concept

The design will support easy installation by transit service maintenance or contracted personnel. No special skills except knowledge of the interfacing platform's power system will be required.

Maintenance requirements for the system will be minimal. Each unit will include basic self test mechanisms to indicate proper operation visually (e.g. through the use of LEDs). System design allow for easy replacement of defective unit by a new unit with no need for user level maintenance. Defective systems will be returned to the manufacturer for disposition.

No user installed spare parts are expected. Memory cards, if used to meet storage requirements, will be compatible with existing commercially available formats.

2. Threat

Public transportation systems continue to be targets of terrorist attacks. Recent attacks including London (2005), Madrid (2004), and elsewhere around the world demonstrate a general persistent terrorist threat to mass transit systems. In particular, transit systems provide a potentially attractive target to terrorists by virtue of their access to large populations with currently less restrictive access controls than airline and other transportation methods.

3. Existing System Shortfalls

Existing video surveillance systems provide a variety of technical capabilities including systems that meet or exceed specific technical capabilities required herein. However, system and supporting infrastructure costs and maintenance requirements for these systems are often high enough that implementation and system coverage has been limited, thereby reducing the system-wide surveillance capability.

Existing fixed systems include those placed in stations, in tunnels, on bridges, and at access control points. These systems typically rely on a hardwired infrastructure to transmit data away from the point of interest for storage, processing, and commonly viewing. Onsite backup storage is optional but is not often employed. In cases where onsite backup is employed currently, the level of protection in the event of a terrorist attack is largely unknown.

4. Capabilities Required

4.1. Operational Performance Parameters (T: Threshold / O: Objective)

4.1.1. Form Factor

Each BRAVE unit will occupy a volume of less than 3” by 3” by 2” (T) 2” x 2” x 1.5” (O).

4.1.2. Resolution

The system will record and store color video data at a resolution of at least 1CIF (T) / 4 CIF (O).

4.1.3. Frame Rate

Video data recorded and stored by BRAVE will have a frame rate of at least 7.5 FPS (T) / 30 FPS (O). The frame rate will be adjustable at time of installation (O).

4.1.4. Field of View/Focal Length:

The system will be capable of recording video at focal lengths ranging from 3 to 50 ft. Focal length will be set at installation (T) / adjust automatically (O).

4.1.5. Data Format

Video data will be stored in a format in a manner suitable to meet evidentiary requirements (T/O). Recorded data will include a calibrated time stamp that can be used during data retrieval and review (T/O). The system will produce a message digest or “digital fingerprint” of recorded data using cryptographic hash function MD5 or SHA-1 (T/O) to assist in preserving the evidentiary status of the recorded data. Stored videos shall be accessible with standard commercial and open source video playback software (O).

4.1.6. Tamper Resistance

BRAVE units will be constructed to prevent unauthorized access to stored data, device power, and device activation mechanism (T/O).

4.1.7. Power Source

BRAVE units will be compatible with 48V DC, 120 AC, and 12V DC power sources and include any necessary transformer with the system (T) Device will provide self-contained power capability (e.g. solar cells) (O)

4.1.8. Environmental

BRAVE will demonstrate capability to perform within the full range of environmental conditions without degraded performance. System will meet all environmental requirements specified in IEEE 1478 Standard for Environmental Conditions for Transit Rail Car Electronic Equipment for the E3 (Vehicle Exterior, Body Mounted) and E4 (Vehicle Interior, Non-Conditioned) environments.

- Temperature: In addition to the requirements of IEEE 1478, the system will experience no degraded performance due to rapid changes in temperature of 20°C
- Dust: Blowing sand and dust testing will include testing with steel sand and dust particulates

Example Only

- EMI/EMC: System performance will not be degraded due to electromagnetic interference from external devices

4.1.9 Blast Survivability

The BRAVE memory component will demonstrate a capability for stored data to survive a blast for the purposes of reading video imagery. Parameters for this section will be provided separately.

4.2. Key Performance Parameters (KPPs)

4.2.1. Cost

Individual unit cost will not exceed \$200 (T) / \$100 (O) based on production quantities of 100,000 or more. Costs of support equipment and software to operate and access data on individual surveillance units will not exceed \$1,000 (T) / \$0 (O) per 100 units in use.

4.2.2. Storage Capacity

Data storage will be sufficient for data storage of continuous video recording for a period of 7 days (T) / 14 days (O).

4.3 System Performance.

4.3.1 Mission Scenarios

BRAVE units will be located on mass transit vehicles or infrastructure (e.g. tunnels and bridges). Units will be installed to continuously monitor a designated area with minimal human intervention required until data retrieval or unit replacement is required. BRAVE will operate in a range of environmental conditions including large temperature swings, humidity, rainfall, vibration/shock, dust, and EMI/EMC considerations. Units will also be capable of recording in low light conditions.

In the event of a terrorist attack, when catastrophic data retrieval is required, video storage will be recovered and transferred from the potentially damaged housing of the units of interest. Recorded video data will be reviewed and analyzed as part of the forensic investigation as appropriate.

In non-catastrophic data retrieval scenarios, such as data use in a criminal investigation or forensic investigation from a unit not damaged by the attack; the unit housing and electronics will be reused. In these cases, the operator will remove the current memory card, taking care to document the proper chain of evidence, and replace it with a new unused memory card.

Periodic visual checks of the system's self diagnostic indicator will be conducted by operators or maintenance personnel. Minimal training of personnel is required to ensure proper understanding of system self diagnostic indicators.

Example Only

4.3.2 Interoperability

Recorded data will be compatible with existing commercial and open source file formats including MPEG2, MPEG4 or H264 (T/O). Stored videos shall be accessible with standard commercial and open source video playback software (O)

4.3.3 Human Interface Requirements

Once installed, direct human interface with the system will not be required except for data retrieval. Installation will require basic mechanical skills to attach and position the unit. Knowledge of the interfacing power system will also be required. Data access and retrieval will require basic to intermediate computer skills and familiarity with using memory cards or USB storage mediums (dependant of final design).

Human interface is also required to periodically check maintenance self check indicators. If needed, unit replacement will require similar skills to installation.

4.3.4 Logistics and Readiness

The system is required to be operational for long periods of continuous operation without interruption. No user level maintenance or spare part replacement is required. Replacement units and memory cards should be available in case replacement is required.

Mean Time Between Failures (MTBF): 40,000 hours (T) 80,000 hours (O)

5. System Support

5.1 Maintenance

Each BRAVE unit will have the capability to visually indicate to a minimally trained individual that it is no longer functioning and needs repairs or replacement. User level maintenance shall be limited to monitoring of self diagnostic indicator and installation, removal and replacement of the system. All other maintenance will be vendor provided as necessary.

5.2 Supply

No special tools or support equipment are required for installation or replacement. Manuals will be provided to the operator by the vendor and will include installation procedures, information on diagnostic indicators of unit self test, and replacement procedures. Manual will also provide information on routine and catastrophic (i.e. after a terrorist attack) data retrieval.

5.3 Support Equipment

All self test diagnostic tests will be contained within the unit. No external support equipment will be required to maintain and operate the unit. Suitable computer equipment will be required to review data retrieved from the system. Specific hardware and software requirements will depend on the level of analysis to be conducted and the quantity of video data to be analyzed.

Example Only

5.4 Training

Users will be instructed on the installation and replacement of units; interpretation of self test diagnostic indicators; and data retrieval procedures by manuals and written procedures supplied by the unit manufacturer.

5.5 Transportation and Facilities

Once installed, individual units will remain in place until removed or replaced. Transportation of individual units for installation or replacement is expected to be well within individual carriage limitations and will be dependent on the local installation point.

Transportation of retrieved digital media will require no special technical capability but should be conducted consistent with applicable procedures to preserve chain of custody when data retrieval is conducted for use in legal proceedings (e.g. criminal prosecution or civil litigation).

Facilities and suitably computer equipment will be required to review data retrieved from the system. Facility sophistication and size will depend on the level of analysis to be conducted and the quantity of video data to be analyzed.

6. Force Structure

Video surveillance cameras are typically positioned on vehicles to cover each entrance and the length of the vehicle in each direction. Cameras can also be positioned to show vehicle exteriors. Each standard bus is expected to make use a minimum of 4 units. Longer articulated buses will use 7 or more units, while Train cars can make use of 6 or more units. Based on current public transportation fleet size and current video surveillance usage rates, approximately 200,000 – 300,000 units would be required to provide the discussed video surveillance capability to mass transit vehicles without a current video surveillance capability.

Additional systems will be required within each locality based upon the demonstrated reliability rate to ensure that replacement systems are on hand for quick replacement of faulty units. An additional quantity of the appropriate removable memory cards will be necessary as well, to ensure availability of replacement cards when data is removed for forensic and other purposes.

Additional systems may be required for in station, infrastructure, and other surveillance purposes.

7. Schedule

Demonstration of an initial operational capability is required within 4 (T) / 3 (O) months. For the purpose of this effort, initial operational capability is defined as installation and field demonstration of 100 fully operational units will include in an identified major city transit system.

8. System Affordability

Individual unit cost will not exceed \$200 (T) / \$100 (O) based on production quantities of 100,000 or more. Costs of support equipment and software to operate and access data on individual surveillance units will not exceed \$1,000 (T) / \$0 (O) per 100 units in use.

Operational Requirements Document

Predictive Modeling for Counter-Improvised Explosive Devices

Contents

1. General Description of Operational Capability	264
1.1. Capability Gap	264
1.2. Overall Mission Area Description	264
1.3. Description of the Proposed Product or System.....	265
1.4. Supporting Analysis	265
1.5. Mission the Proposed System Will Accomplish	265
1.6. Operational and Support Concept.....	266
1.6.1. Concept of Operations	266
1.6.2. Support Concept	267
2. Threat	267
3. Existing System Shortfalls.....	268
4. Capabilities Required	269
4.1. Operational Performance Parameters.....	269
4.2. Key Performance Parameters (KPPs).....	270
4.3 System Performance.....	270
4.3.1 Mission Scenarios	270
4.3.2 System Performance Parameters	271
4.3.3 Interoperability	271
4.3.4 Human Interface Requirements.....	271
4.3.5 Logistics and Readiness	271
5. System Support	272
5.1 Maintenance	272
5.2 Supply.....	272
5.3 Support Equipment.....	272
5.4 Training.....	272
5.5 Transportation and Facilities.....	272
6. Force Structure.....	272
7. Schedule	273
8. System Affordability	273

1. General Description of Operational Capability

1.1. Capability Gap

This operational requirements document (ORD) addresses the capability to predict the threat of an IED attack, identified by the Counter-IED Capstone IPT. It also covers a number of technology needs identified to further data fusion from law enforcement, intelligence partners and other sources to support the common operating picture.

1.2. Overall Mission Area Description

The Department of Homeland Security (DHS) plays a major role in fulfilling Presidential Directive/HSPD-19 (Combating Terrorist Use of Explosives in the United States) including national policies, strategies and implementation plans for the prevention and detection of, protection against and response to terrorist use of explosives in the United States.

Terrorists have repeatedly shown their willingness and ability to use explosives as weapons worldwide and there is ample intelligence to support the conclusion that they will continue to use such devices to inflict harm. The threat of explosive attacks in the United States is of great concern considering terrorists' ability to make, obtain, and use explosives, the ready availability of components used in IED construction, the relative technological ease with which an IED can be fashioned and the nature of our free society.

It is the policy of the United States Government to counter the threat of explosive attacks aggressively by coordinating Federal, state, local, territorial, and tribal government efforts and collaborating with the owners and operators of critical infrastructure and key resources to deter, prevent, detect, protect against and respond to explosive attacks, including the following:

- (a) Apply techniques of psychological and behavioral sciences, such as social network theory, in the analysis of potential threats of explosive attack;
- (b) Use the most effective technologies, capabilities, and explosives search procedures and applications to detect, locate and render safe explosives before they detonate or function as part of an explosive attack, including detection of explosive materials and precursor chemicals used to make improvised explosive or incendiary mixtures;
- (c) Apply all appropriate resources to pre-blast or pre-functioning search and render-safe procedures, and to post-blast or post-functioning investigatory and search activities, in order to detect secondary and tertiary explosives and for the purposes of attribution;

Example Only

- (d) Employ effective capabilities, technologies and methodologies, including blast mitigation techniques, to mitigate or neutralize the physical effects of an explosive attack on human life, critical infrastructure, and key resources; and
- (e) Clarify specific roles and responsibilities of agencies and heads of agencies through all phases of incident management from prevention and protection through response and recovery.

1.3. Description of the Proposed Product or System

The proposed solution shall employ the knowledge and understanding gained in the military environments such as Iraq and Afghanistan to model and take action against IED network activities in the United States. It shall enable investigators to disrupt networks by expanding analysis and investigation beyond the groups and individuals that place devices to analyze and target the finances, materiel and supply line of parts, and “the brains” that build and deploy IEDs. DHS knows that the insurgents who seek to place IEDs in the United States (as they do in other parts of the world) are often supported by organized networks that finance their operations, supply critical elements for the production of IEDs, create the devices and plan and execute attacks. The proposed solution shall implement powerful analytics to gain critical, data-driven insight into the structure, character, interactions and methods associated with those networks. By analyzing data from a myriad of sources, the new solution shall identify and analyze the linkages between individuals and groups that may indicate a support network.

1.4. Supporting Analysis

DHS has undertaken an array of activities designed to prevent the detonation of IED/VB-IED/suicide bombs inside the United States and against American interests abroad. The department is aggressively working to focus on identifying and attacking the threat before terrorists have the capability to detonate a device. That begins with attacking the foundation of the threat—the social, operational and financial networks. Critical to the efforts is developing an integrated, cross-agency data-driven foundation of intelligence as the basis for deterring and incapacitating those who supply/obtain the funds for IEDs, identifying the organization planning to manufacture and plant the IED and intercepting the gathering and procurement of materials for the IED.

1.5. Mission the Proposed System Will Accomplish

The proposed solutions is envisioned to be a seamless, transparent and an integrated combination of COTS software, training and services that form an intelligence collection and analysis system that will help uncover and target the operational, financial and social networks involved in IED deployment in the United States. The solution shall address the challenges of data access, integration, quality and management of data coming from multiple government agencies and publicly available sources. In the modern and developed world, where most of the explosives/IED support networks operate, government agencies and the private sector generate unprecedented volumes of data. Customer profiles, organizational operational performance and personal behavior of individuals are monitored by multiple service providers. Some data resides in structured form in databases or

Example Only

exists as real-time streams. Some exists in unstructured form, for example as e-mails, electronic documents or media files. Whatever the form, there exists potential to transform these data into relevant intelligence to improve investigative decision-making. A proposed solution shall integrate existing data from all relevant sources, and with its advanced analytics and reporting capabilities, provide actionable information to U.S. investigators in the full range of Federal, state, local and tribal jurisdictions.

This must be a cross-agency solution that is designed to deliver a broad range of intelligence products within a multi-level environment (Federal, state, local and tribal jurisdictions) to provide the full community of decision makers, analysts and investigators with better information to address potential threats.

Because first responders are an integral part of a tactical, pre-initiation response to an immediate threat, the proposed solution must address the appropriate type and level of information that would support those contingencies and how that information would be shared at the first responder level.

A proposed solution can use an integrated suite of tools, including but not limited to data integration and management, data and text analysis, predictive modeling and optimization and social network analysis coupled with link analysis. Analysts and other end users will receive detailed intelligence developed using data driven investigative techniques and link analysis based on social network theory. Analysts will be provided with client tools, such as customizable report creation and delivery capabilities that provide intelligence in the most appropriate format for decision makers and other users. The solution can be customizable, if desired, at all levels of security classification. The data will be searchable via a graphic user interface that will allow the investigator/analyst team to search for unusual behaviors and complex sequences of behaviors across records.

1.6. Operational and Support Concept

1.6.1. Concept of Operations

A solution will bring together key elements of intelligence needed to enable analysts, investigators and decision makers to make data driven decisions to more effectively perform their mission.

Specifically, the proposed solution shall:

- Link disparate, cross-agency data sources and integrate required elements
- Enhance data quality and accuracy
- Develop information across large volumes of integrated data
- Use data/text mining, predictive modeling and other advanced analytics methodology to provide insight to relevant data
- Expediently operationalize intelligence
- Identify suspicious social, financial and operational networks that may be appropriate for further analysis or investigation
- Communicate actionable information out to decision makers and investigators via the Internet, LAN/WAN, email, etc.
- Enable the agency to better detect and defeat potentially dangerous networks

Example Only

A solution must integrate the efforts of analysts and decision makers at a cross-department/cross-agency level in a “fusion center” type environment. Sources of record will be made available so that the solution can automatically pull data on a near real time basis to update the intelligence available. A proposed solution will work within the specified DHS IT environment and will pull data from existing systems. Access to data sources will be granted by the responsible agency.

1.6.2. Support Concept

The responsible department/agency will consider options for the implementation and sustainability of the proposed solution.

The data integration and management, along with the analysis and modeling, social network development, linking and scoring functions shall be maintained at the agency level, with analysis and reports made available over the appropriate networks to users based on role or persona. Analysts, based on their role and mission requirements, will be given additional analytical capabilities to better perform their responsibilities.

A proposed solution will support the full range of services required for sustainability of the system. This shall include data integration and cleansing, data and text mining, predictive modeling, social network development linking and scoring. A solution will include proposed actions that the agency could take to develop the appropriate skills within the organization, particularly those related to data extraction, cleansing, integration and intelligent storage.

Training in the operation of the system, both for the initial implementation and for long term sustainability, shall be provided as part of the solution, as well as tailored courses, delivered on site, that focus on specific agency issues and requirements.

2. Threat

The potential threat to the United States from improvised explosive devices, vehicle-borne IED (car bombs) and suicide bombers is well established. Incidents since the beginning of 2000 in Bali, Madrid, London, Libya, as well as the attacks on the U.S. in Oklahoma City on 19 April 1995 and the World Trade Center bombing on 26 February 1993 attest to the potential threat and difficulty in protecting against them. This is not a new phenomenon, as seen in the actions of the Red Brigade and Bader-Meinhof Gang directed against U.S. interests in Europe in the mid 1970, the attack on the U.S. Marine Barracks in Beirut in 1983 and others. Current intelligence and law enforcement estimates predict that these types of attacks against the population of the United States are inevitable.

Specific types of attacks could be the type of IED/VB-IED/suicide bombing widely employed in current combat zones and around the world, but could also include use of explosive devices combined with commercially available, stolen or smuggled biological, chemical or radiological agents to cause further loss of life, widespread panic and economic damage.

Example Only

Nearly every incident of IED/VB-IED/suicide bombing involves groups or networks of individuals acting in concert. While these networks may vary in type and complexity, they have common characteristics, such as the need to communicate, fund operations, procure materiel and travel to accomplish their objectives. These activities leave transactional records in databases legally maintained by government and commercial entities. By leveraging and extending insight into these data sources, it is possible to assemble a threat profile to protect against future attacks.

3. Existing System Shortfalls

Current systems fall short in the following areas:

- a) Lack of the capability to integrate data from disparate sources. Data is contained in multiple systems within disparate organizations. It is often on different platforms and in different environments with different security and access requirements. Some is in transactional systems such as Oracle, SAP, DB2, Microsoft desktop applications and others, some in proprietary databases, some in legacy systems built in FORTRAN, COBOL or ADA. Integrating the sources is a complex technical problem, complicated by the various internal departmental/agency policy and cultural issues.
- b) Volume of data to be analyzed. Not only is data in various agencies, formats, platforms and environments, the amount of data that should be considered in a comprehensive program is quite substantial, with gigabytes if not terabytes available for analysis. Since many of the transactional sources are updated in real time and others on a daily basis, the volume of raw data to be extracted, integrated and analyzed as required to provide timely, actionable information to analysts and investigators is a significant challenge.
- c) Solutions lack scalability and robustness. Current less-flexible and less-capable systems have issues such as how new agencies or data sources can be incorporated into the data integration regime. Because current solutions are typically single agency efforts, the requirements for scalability and robustness are typically not addressed.
- d) Lack of advanced analytics. Agencies typically do not have the capability to apply high end or advanced analytics, such as data indexing and profiling, data and text mining, predictive modeling, forecasting and optimization to their mission requirements. The types of network analysis and network linking required cannot be accomplished using multiple purpose, less sophisticated technology.
- e) Absence of a foundation in social network theory. Department/agency personnel do not have a thorough grounding in the theory of how social networks interact and change patterns of behavior. This hampers their ability to gain maximum intelligence from existing data. The use of social network theory domain experts, thought leaders,

Example Only

academicians, investigators and analysts, operating within the appropriate technology environment is not optimal.

4. Capabilities Required

4.1. Operational Performance Parameters

The performance metrics included as part of the Threshold (T) and Objective (O) Values are based on 10 government data sources, 300 total users – 50 of them concurrent – located in 3 locations within the United States.

		Objective Value	Threshold Value
1		Data Integration	
	a	Integrate, cleanse and store data from multiple sources.	Demonstrate the capability to perform the objective within 4 hours in 100% of the identified requirements.
	b	Pull data on a schedule from disparate data sources	Demonstrate the capability to perform the objective within 1 hour in 100% of the identified requirements.
	c	Conduct data cleansing and initial profiling as appropriate	Demonstrate the capability to perform the objective within 2 hours in 100% of the identified requirements.
	d	Write the data into a data warehouse	Demonstrate the capability to perform the objective within 1 hour in 100% of the identified requirements.
	e	Create a metadata repository with full bi-directional linkages with all Data Integration, Reporting, Data Visualization and Advanced Analytics components	Demonstrate the capability to perform the objective within 1 hour in 100% of the identified requirements.
2		Conduct analysis on the data available. This includes indexing and profiling, integrated data and text mining, predictive modeling, forecasting and optimization as required to meet mission requirements	Demonstrate the capability to perform the objective within 2 hours in 100% of the identified requirements.
3		Develop networks , along with soft and hard links, based on the data provided	Demonstrate the capability to perform the objective within 4 hours in 100% of the identified requirements.

Example Only

4	Score the networks as benign or suspicious based on criteria established by the PM	Demonstrate the capability to perform the objective within 2 hours in 100% of the identified requirements.
5	Identify and list key network behaviors and potential vulnerabilities	Demonstrate the capability to perform the objective within 2 hours in 100% of the identified requirements.
6	Push information out to end users in multiple formats (portal, PDA, reports, alerts, etc) based on responsibilities, roles and access rights	Within 4 hours of completion of analysis and upon release by the appropriate authority
7	Provide standard interactive, parameterized “What if” interfaces for end users based upon model outcomes and parameters.	Interfaces updated with latest models and parameters within 4 hours of completion of analysis and upon release by the appropriate authority
8	Provide controlled data access via system metadata layer for ad-hoc, reporting, data visualization, and advanced analytic modeling to end users based on responsibilities roles and access rights.	Within 4 hours of completion of analysis and upon release by the appropriate authority
9	Provide integrated accuracy monitoring of “predicted” versus “verified” condition monitoring of scoring outcomes with threshold triggers to recalibrate or redevelop scoring algorithms.	Demonstrate the capability to perform the objective within 2 hours of the completion of scoring activities.

4.2. Key Performance Parameters (KPPs)

All Operational Performance Parameters are considered mandatory.

4.3 System Performance.

4.3.1 Mission Scenarios

The purpose of a solution is to provide analysts, investigators and decision makers the ability to gain more thorough and detailed insight of cross-agency data, using proven COTS technology, to better identify potential threats to the United States.

The solution shall be deployable into a cross-agency headquarters level environment operating at a minimum SECRET classified level. The three primary purposes of a solution are to:

Example Only

- Extract, cleanse and integrate data from Federal, state, local and tribal agencies into a data repository, staged for the application of advanced analytics. Data must be accessed from a range of transactional, operational and individual sources in a variety of software platforms residing in different environments with operating systems with various levels of classification, potentially worldwide.
- Apply advanced analytics to develop data-driven intelligence on social, operational and financial networks potentially involved in domestic IED/VB-IED/suicide bomb attacks on the United States. The term “advanced analytics” is interpreted to include but is not limited to the use of text and data mining, predictive modeling, forecasting and optimization, within the context of innovative thought leadership to develop the most comprehensive and integrated understanding of a given threat, as well as how to validate and respond to it.
- Communicate the analytic results to decision makers, analysts and investigators within the appropriate cross-departmental environment for action. Information and intelligence should be available in a variety of outputs. Access and permissions must be based on roles and responsibilities.

4.3.2 System Performance Parameters

The Performance Parameters are addressed above in Section 4.1

4.3.3 Interoperability

- Interoperability, defined as the capability of applications to exchange information and to operate cooperatively using this information, is a critical aspect of this solution, since data will be integrated from disparate sources through the Federal, state, local and tribal infrastructure. The solution must sit atop the systems identified by the department/agency and extract, cleanse and load to a data warehouse or repository (or potentially multiple repositories) with minimal human interaction and full transparency, the ability to audit, read and write in native language to the source systems is also required. A solution shall reduce overhead and make access to the required sources and data elements efficient and timely.

4.3.4 Human Interface Requirements

A solution shall operate in a controlled, IT-type environment at a department/agency owned or contracted facility within the United States. The solution shall comply with all Federal core configuration requirements.

4.3.5 Logistics and Readiness

- A solution shall include both production and backup architecture to ensure the solution maintains at least a 99% rate with a ≤ 3 hours resumption of service capability in case of catastrophic failure.
- Logistics (maintenance and supply) requirements are addressed below in Sections 5.1 and 5.2

5. System Support

5.1 Maintenance

Maintenance of the hardware for the hosting system shall be the responsibility of the department/agency. Maintenance of the technology platform, including resolution of technical support issues and installation of upgrades or fixes, will be the responsibility of the solution provider.

5.2 Supply

The operating environment—including a combination of separate development, test, production and backup environments—will be operated and maintained by the department/agency with solution-specific supplies or spares for sustained operation with 99% availability.

A solution will include both system and agency-specific solution documentation, tailored for agency use and delivered both online and as standalone media (CD/DVD or thumb drive), in required.

5.3 Support Equipment

A solution shall require support equipment that is readily available as commercial-off-the-shelf equipment.

5.4 Training

A solution shall provide for the full range of training needed to operate the system and provide the services required at Technology Readiness Level (TRL) 9. A solution will specify the specific training provided to ensure that users are capable of operating and using a proposed system. It will identify the training required for each component of the overall solution along with metrics to verify that each person participating in the training is certified upon completion.

A solution will make use of online and self-paced learning modes, but, where appropriate, provide for classroom training. Classroom training should be tailored to the needs of the agency-specific solution and be conducted training facilities provided by the agency.

Training materials will be provided, in electronic format—online or via portable media—for all courses, including online or distance learning modules.

5.5 Transportation and Facilities

A solution will be hosted in a government-specified, controlled environment with no anticipated requirement for transportation.

6. Force Structure

A solution must consist of COTS software deployed in development, test, production and backup environments, with the required hardware sets provided by the government. The development and test environments will be used to tailor a production-ready, COTS technology platform to ensure that the environment

Example Only

available to the end user community is at TRL 9. The environments could be separately located.

The system shall be certified for use at least at the SECRET classified level and operate in both the unclassified and classified environments with the appropriate safeguards in place.

The solution should scale to accept classified and unclassified data feeds from an unlimited number of sources, regardless of the host operating system or base application. In addition, the solution should accommodate manual input from unlimited number of users via the Internet or WAN/LAN, as well as an unlimited number of end user via the same connectivity.

7. Schedule

A solution will be at TRL 9 within 6 months from the day access to the identified data sources is confirmed by the agency Program Manager and the solution provider.

TRL 9 is generally defined as the ability to do the following:

- Link disparate, cross-agency data sources and integrate required elements into a data warehouse/repository with a supporting metadata layer
- Enhance data consistency and accuracy using data quality/cleansing software
- Use data/text mining, predictive modeling and other advanced analytics methodology to provide insight to relevant data
- Identify suspicious social, financial and operational networks that may be appropriate for further analysis or investigation
- Push actionable information out to decision makers and investigators via the Internet, LAN/WAN, email, etc.

8. System Affordability

The hardware will be provided by the department/agency and the software component of the solution shall include all technology required for:

- Data integration, cleansing storage and management
- Analytics, including data and text mining, predictive modeling and forecasting
- Development and scoring of social networks
- Deployment of information to end users with a capability to run stored processes from within Microsoft Office desktop applications, do ad hoc query and analysis and drill down
- Full control of access to the solution by a local system administrator
- Full documentation at the system administrators, analysts and end users levels
- 24/7 Technical support

Example Only

Training shall be included for system administrators, analysts and end users in Web-deployed and on-site classroom training packages.

The services component of the solution shall include:

- Installation and configuration of all software, including all fixes and upgrades
- Development of analytical models
- Scoring and linking within the context of the social network models
- Knowledge Transfer to government employees or contract personnel as directed

The total delivered price should be \leq \$500,000 (includes department/agency usage rights). In addition, provide a fixed price proposal for seat or facility licensing fee for users outside of the department/agency.

A conservative estimate of the potential available market is over 250,000 seats in the United States alone. It is conservatively estimated that there are more than 5 Federal departments/agencies identified as potential users for the proposed system.

Appendix C: DHS S&T Infrastructure and Geophysical Division (IGD) Brief

Slide 1

Infrastructure Geophysical Division (IGD)

Overview

Infrastructure and Geophysical Division
Science and Technology Directorate
Department of Homeland Security



Slide 2

DHS Science & Technology Directorate Technical Divisions



EXPLOSIVES

BIOLOGICAL & CHEMICAL

COMMAND, CONTROL & INTEROPERABILITY

BORDERS & MARITIME SECURITY

HUMAN FACTORS

INFRASTRUCTURE & GEOPHYSICAL



2

Slide 3

Basic Research Portfolio

Discovery and Invention to Enable Future Capabilities





- Brings the capabilities, talent and resources of the Homeland Security Centers of Excellence, DOE National Laboratories and DHS Labs to bear to address the long-term R&D needs for DHS in sciences of enduring relevance
- This type of focused, protracted research investment has potential to lead to paradigm shifts in the nation's homeland security capabilities







Homeland Security

3

Slide 4

Innovation Portfolio

High Risk, High Gain, Game Changers for Leap-Ahead Results





- Promotes revolutionary changes in technology
- Focus on prototyping and deploying critical technologies

Includes:

- HSARPA – Homeland Security Advanced Research Projects Agency
Visit <https://baa.st.dhs.gov>
- Small Business Innovation Research program
Visit <http://www.sbir.dhs.gov>

DHS S&T Solicitations also posted at: <http://www.FedBizOpps.gov>







Homeland Security

4

Slide 5

Product Transition Portfolio

Enabling Capabilities, Supporting Mission Critical Needs of DHS





Integrated Product Teams (IPTs)

- 13 Capstone IPTs form the centerpiece of the S&T's customer-driven approach to product transition
- Engage DHS customers, acquisition partners, S&T technical division heads, and end users in product research, development, transition and acquisition activities
- Identify our customers' needs and enable and transition near-term capabilities for addressing them



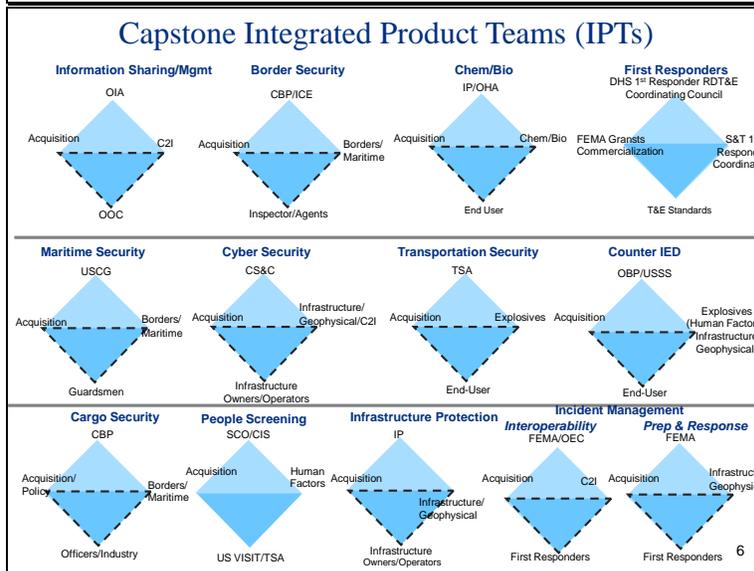




Homeland Security

5

Slide 6



Slide 7

Infrastructure Geophysical Division (IGD) Mission

Infrastructure and Geophysical Division will increase the Nation's **preparedness for and response** to natural and man-made threats through superior situational awareness, enhanced emergency responder capabilities, and **critical infrastructure protection**



Homeland Security

7

Slide 8

The IGD Transition Business Model

- ▶ **Customer driven**
 - Office of Infrastructure Protection (IP)
 - Federal Emergency Management Agency (FEMA)

- ▶ **User oriented**
 - Infrastructure owners and operators
 - First responders and emergency managers

Homeland Security
8

Pay attention to specific parameters in order for owners and operators to embrace technology
 OIP has good relationship/mechanism to getting to customer base
 FEMA has relationship with U.S. Fire Administration

Slide 9

Infrastructure Protection Collaboration & Coordination

The DHS Office of Infrastructure Protection (IP) serves as the bridge between the 18 CIKR Sectors and the DHS Science and Technology Directorate

R&D needs

critical infrastructure protection technologies

- 18 CIKR Sectors
 - Sector Specific Agencies
 - Sector Coordinating Councils
 - Government Coordinating Councils
 - Office of Infrastructure Protection Divisions
 - Office for Bombing Prevention

- DHS Science and Technology
 - IP led or co-led Capstone IPTs
 - Infrastructure Protection Capstone IPT
 - Chemical and Biological Defense Capstone IPT
 - Counter-IED Capstone IPT

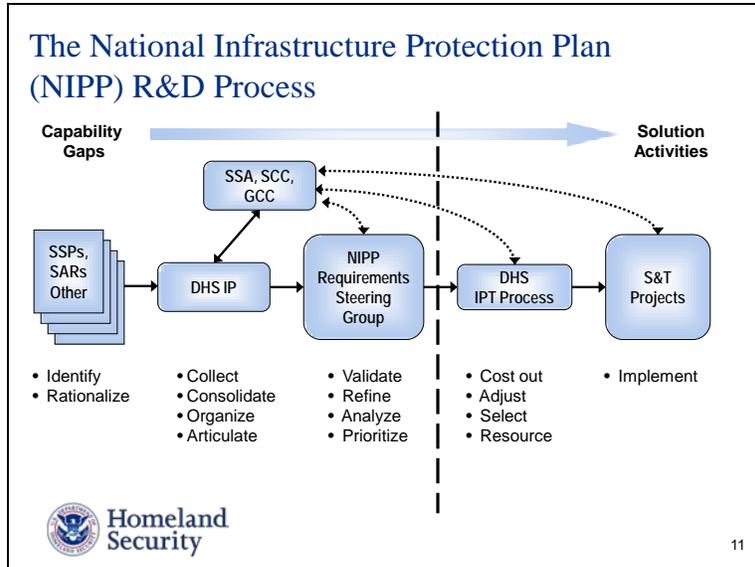
Homeland Security
9

Slide 10

Critical Infrastructure Sectors & Lead Agencies

Sector-Specific Agency	Sector
Department of Agriculture Department of Health and Human Services	Agriculture and Food
Department of Defense	Defense Industrial Base
Department of Energy	Energy
Department of Health and Human Services	Public Health and Healthcare
Department of Interior	National Monuments and Icons
Department of Treasury	Banking and Finance
Environmental Protection Agency	Water
Department of Homeland Security Office of Infrastructure Protection	Chemical Commercial Facilities Dams Emergency Services Nuclear Reactors, Materials, and Waste Critical Manufacturing
Office of Cyber Security and Telecommunications	Information Technology Communications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration, United States Coast Guard	Transportation Systems
Immigration and Customs Enforcement, Federal Protective Service	Government Facilities

Slide 11



Slide 12

IGD Thrust Areas

- ▶ Infrastructure Protection (IP)
- ▶ Preparedness and Response
- ▶ Geophysical Sciences

The slide includes three images: a map of the United States with various infrastructure icons (power lines, bridges, etc.), a photograph of three police officers in uniform reviewing a document, and a satellite image of a hurricane.

Homeland Security logo is at the bottom left. The number **12** is at the bottom right.

Slide 13

IGD Preparedness and Response (P&R) Program Areas

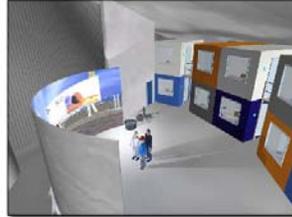
- ▶ Integrated modeling, mapping, and simulation
- ▶ Personnel Monitoring
- ▶ Incident management enterprise system
- ▶ Logistics management tool

The slide includes two images: a photograph of emergency responders in full gear (hard hats, reflective vests) and a 3D network diagram showing nodes and connections, with text labels like '3D Network System', 'First Node', 'Response in 3D Space', and 'Real-time Network in 3D Space'.

Homeland Security logo is at the bottom left. The number **13** is at the bottom right.

Slide 14

P&R: Training, Exercise and Lessons Learned (TELL)



14

Simulation driven virtual/live/constructive emergency response exercise (USAR slide) Decision making (EOC Slide) , consequences, and causes and effects analysis (virtual training room slide)

Slide 15

P&R: Unified Incident Command and Decision Support (UICDS)



Unified Incident Command and Decision Support (UICDS)

Open-architecture Framework (EOC slide) Gather and share mission critical information (police slide) Manage resources and seamlessly communicate (Fire slide) Scale from local incidents to incidents of national significance (FEMA USAR Slide)

Slide 16

P&R: Regional Technology Integration (RTI)



6

Deploy innovative technologies across the nation in multi-county/multi state large urban areas

Slide 17

P&R: Personal Protective Equipment

The diagram illustrates the layers of the P&R equipment: Durable Outer Shell, Water Repellent Finish, Flame Resistant Aramid Woven Rip Stop, PTFE Nanoporous Membrane, AirWeld Seals, Activated Carbon, Reactive Nanoparticulates & Polyconjugates, Flame Resistant Inner Lining Fabric, and a Replaceable Adsorptive/Reactive Liner. Photos show personnel in blue and white protective suits in various operational settings.

Homeland Security

17

Slide 18

P&R: Escape Hood

The photo shows a person wearing a clear escape hood with a white face mask. The 3D model shows a rectangular hood with a circular red filter on the front and a handle on top.

The concealable mask

Homeland Security

18

Slide 19

P&R: 3-D Locator

The photo shows a person in a control room with multiple computer monitors. The 3D diagram shows a building with floors labeled 3rd floor, 2nd floor, 1st floor, and basement. A network of nodes (a, b, c, d, e) is shown within the building, with a text box stating 'No GPS signal in this level'. A 'Tier 1 Network in Building' is also indicated. A fire truck and a police car are shown at the bottom, with a text box stating '3D Locator System Finds Node Positions in 3D Space'.

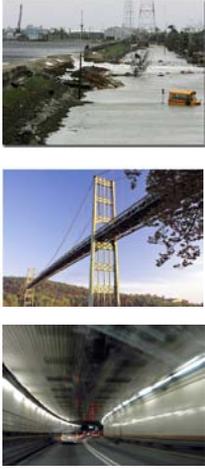
Homeland Security

Deploy innovative technologies across the nation in multi-county/multi state large urban areas

Slide 20

IGD Infrastructure Protection (IP) Program Areas

- ▶ Interdependencies and cascading consequences
- ▶ Blast analysis and protection
- ▶ Advance surveillance
- ▶ Rapid mitigation and recovery
- ▶ Critical utility components
- ▶ Community based critical infrastructure protection institute

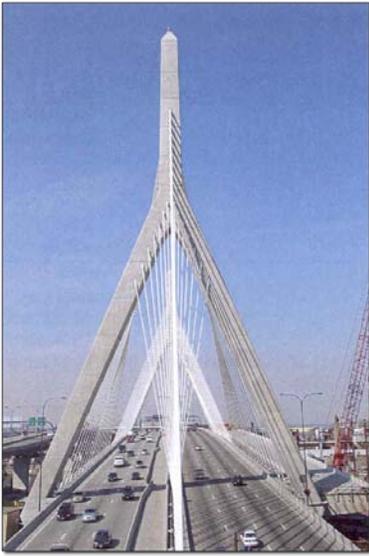



20

Blast analysis – counter IED effort

Slide 21

IP: Mitigation for Cable-Stayed Bridges Subjected to Near-Contact Explosives



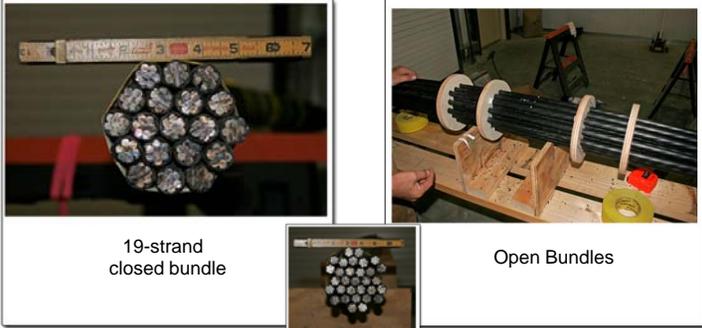

Focus: Cable-Stayed Bridges
Problem: These bridges are highly vulnerable to detonations adjacent to the towers or attack on the cables.

Current research focuses on two components:
Cables exposed to IEDs
Towers exposed to VBIEDs

For both components, research will address:
Baseline vulnerabilities
Mitigation schemes using current state-of-the-art
Validity of current analytical models

Slide 22

IP: Un-Protected Cables Baseline Vulnerability Tests



19-strand closed bundle

31-strand closed bundle

Open Bundles



22

Slide 23

IP: Levee Strengthening & Rapid Repair



23

This program will design, test, evaluate, and develop fast techniques to rapidly stop a breach in a levee; (Helicopter slide) advance these techniques to strengthen the levee in substandard areas quickly and before a breach initiates; and, pre-emptively identify problem areas for strengthening or pre-deployment of strengthening measures (Waterway Bridge Slide)

Slide 24

IP: Community Based Technologies



24

Develop and manage a virtual R&D enterprise, involving academia, the private sector, and DHS, that addresses the Nation's critical CIP priorities and results in community-based homeland security technologies that can be quickly transitioned to commercialization

Partners: National Institute for Hometown Security (NIHS) and the Kentucky Homeland Security University Consortium

Slide 25

IGD Geophysical Program Areas

- ▶ Southeast Region Research Initiative (SERRI)
- ▶ Rapid Levee Repair
- ▶ Secure Against Fires and Embers (SAFE)



25

Slide 26

Emerging Areas of Interest

- ▶ Cyber-Physical System Security
- ▶ Advanced Materials Research



Slide 27



Homeland Security

Appendix D: Bridging the Communications Gap (Article)

Bridging the “Communications Gap” between the Public and Private Sector – Making it Easier to do Business with DHS

DHS’s new commercialization outreach efforts center on notifying the private sector about opportunities that exist for partnership and business development to address the needs of the Department.

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
Commercialization Office
U.S. Department of Homeland Security

If you think about it, there are numerous examples in our professional and private lives where the lack of communication or unclear terminology has created misunderstandings, problems and myriad other issues. As in any worthwhile pursuit, effective communication is critical in the cost-effective and efficient interactions between various parties seeking a mutually beneficial partnership. The U.S. Department of Homeland Security (DHS) is putting into practice the necessary rigor to improve communication that will allow the public and private sectors to work jointly to meet the unsatisfied needs of the DHS in order to protect the Nation.

To this end, the DHS Commercialization Office has developed a number of processes, programs and tools to facilitate the clear articulation of DHS needs (See Figure 1). In that same spirit of working together with the private sector, we recently developed a “Product Realization Chart” (see Appendix H) which is a useful guide to relate concepts and correlate terminology used by both the public and private sector to clearly delineate how science, technology development and product development (terms used in the private sector) are related to basic research, innovation and transition using a Technology Readiness Level (TRL) “backbone” (terms used in the public sector).

Further examination of the Product Realization Chart shows that this resource also provides a stage-gated approach for cost-effective and efficient product development to provide a “discussion framework” useful in private-public sector discussions as well as a template for utilization to develop and communicate agreements. The chart describes the objectives, deliverables and the type of management review necessary to develop and deliver technologies/products/services that meet the specific requirements of the DHS’ operating components (U.S. Coast Guard, FEMA, TSA, CBP, USCIS, U.S. Secret Service and ICE) and its end users such as first responders.

Stage One: Needs Assessment

Needs assessment is the critical first stage of product realization (accomplished via acquisition or commercialization processes) that enables DHS to identify capability gaps and investigate new product/technology/service capabilities. By understanding the specific and detailed requirements of its customers, the DHS Science & Technology Directorate (DHS S&T) conducts market research and technology scans to find and assess technology-based solutions that could potentially be developed, matured and delivered to DHS end users.

Commercialization programs, processes and tools...

- 1) "Developing Operational Requirements" Guide
- 2) "DHS Implements Commercialization Process" Article
- 3) "Partnership Program Benefits Taxpayers as well as Private and Public Sectors" Article
- 4) SECURE Program and website
- 5) DHS online
- 6) Invited talks to trade conventions, reaching small, medium and large businesses. Efforts also extend to meet with minority, disadvantaged and HUB Zone groups on a regular basis.

Figure 1: Outreach efforts to inform the public on "How to do Business with DHS" are receiving positive feedback from the private sector and media. See the following website for additional information:

Please note that management reviews for both the public and private sector are required to ensure that exit criteria and deliverables are met when discussing public-private programs like the SECURE Program.

The remainder of the chart shows the various key objectives and deliverables for each major phase of product realization. Entrance at any point of the chart is possible and certainly, the overall objective of many projects currently underway at DHS is to obtain widely distributed products or services (where commercialization is key). DHS also sometimes has unique "custom-like" requirements with lower unit-volume potential (normally using the Acquisition model as shown in Figure 2). It also should be noted that in a basic research program, it may certainly not be possible to generate an ORD, as the objective may be the "exploring uncharted territory" rather than the development of products or services for sale to a particular market. For this reason, a dark box is drawn around Stage 1 to indicate that the Product Realization Chart is a multiple-use chart, rather than a concrete process because it simply offers a framework to visualize several processes, some of which (developing custom or widely distributed products/services) require a Needs Assessment.

Stage Two: Science

At the beginning of the second stage, basic principles are observed and reported, and scientific research begins to be translated into applied research and development (R&D). At this stage, a program sponsor and end user/customer have been identified and the mission needs statement, feasibility study and program management visions have been developed.

Once basic principles are observed, practical applications can be invented. Applications are speculative, and there may be no proof or detailed analysis to support the assumptions. In the case of developing products/services, operational requirements analysis has been conducted and operational requirements are applied to functional requirements. A risk management plan has been developed, a program cost analysis has been completed and a preliminary security assessment has been conducted.

As the technology concept and/or application is formulated, active R&D is initiated that results in an analytical and experimental critical function and/or characteristic proof of concept. This includes analytical studies to physically validate the analytical predictions of

separate elements of the technology. A Systems Engineering Management Plan (SEMP), Program Management Plan (PMP) and proof of concept plan are key deliverables and serve as exit criteria for the next stage of product realization.

During the second stage, the private sector normally produces a complete product plan during commercialization that addresses marketing opportunities, financial considerations, design concept and many additional analyses. Sales/Marketing team performs a SWOT (strengths, weaknesses, opportunities, and threats), a scenario analysis and a sales forecast estimate. Research assembles the key IP disclosure submissions. Quality Assurance (QA) generates all safety/standards compliance items, calibration requirements and other quality control specifications.

Management reviews for both the public and private sector are required (in partnership projects or programs) to ensure that exit criteria and deliverables are met.

Stage Three: Technology Development

The third stage of product realization ensues when basic technological components are integrated to establish that they will work together, which is a relatively “low fidelity” analysis when compared with the eventual system. The proof of concept report and functional requirements document have been finalized. The SEMP, Test and Evaluation Master Plan (TEMP), quality assurance plan and other deliverables are revised and updated on a continuous basis.

The basic technological components are then integrated with reasonably realistic supporting elements so it can be tested in a simulated environment. The fidelity of the breadboard technology increases significantly in this case. The Operational Requirements Document (ORD) and CONOPS are better developed. The technology scan and market survey are ongoing during the third stage, and an analysis of alternatives is provided.

Once the component is validated in a relevant environment, the system/subsystem model or prototype is demonstrated in a relevant environment. After successful T&E in a simulated operational environment, a preliminary Technology Transition Agreement (TTA) or a Technology Commercialization Agreement (TCA) is executed as applicable. A program manager is identified and an interoperability assessment is performed.

During this stage, the private sector uses its product plan to conduct a beta design review, produce a detailed supplier list and supplier benchmark, begin writing the user’s manual, develop a service strategy, and confirm the risk analysis and review engineering change orders. Manufacturing creates a preliminary manufacturing plan and works with Marketing/Sales to finalize product packaging. Quality Assurance defines regulatory requirements, prepares a preliminary quality plan and procedure for first prototype testing and designs the inspection tooling.

Management reviews for both the public and private sector are required to ensure that exit criteria and deliverables are met.

Acquisition versus Commercialization

Once a representative model or prototype system, which beyond TRL 5, is tested in a relevant environment, the product realization process splits into two paths that are

extraordinarily different as evidenced in Figure 2: Acquisition and Commercialization. Acquisition occurs when a government contractor executes design, development and production, driven by DHS requirements, using DHS funding and under contract to DHS. In this case, the product is then deployed to captive users and the product unit price is determined by cost-based pricing. The contractor's customer is DHS and not the end-user community.

Commercialization, on the other hand, is a private-sector driven activity enterprise that executes design, development and production, driven by market requirements, using private funding and perhaps assisted by DHS technology licenses, standards and grants. The product is then sold as commercial-of-the-shelf (COTS) directly to end users and the product unit price is determined by market-based pricing. The vendor's major customer is the end-user community (e.g. first responders) as well as various private sector markets.

Why is there a need for commercialization? As previously mentioned, DHS requirements, in most instances are characterized by the need for widely distributed COTS products. Oftentimes, the need is for thousands, if not millions of products for DHS' seven operating components and the fragmented, yet substantial first responder end-user market. Figure 2 shows the major differences between a "pure" Acquisition versus "pure" commercialization processes, along with the recently developed and implemented DHS "hybrid" commercialization process.

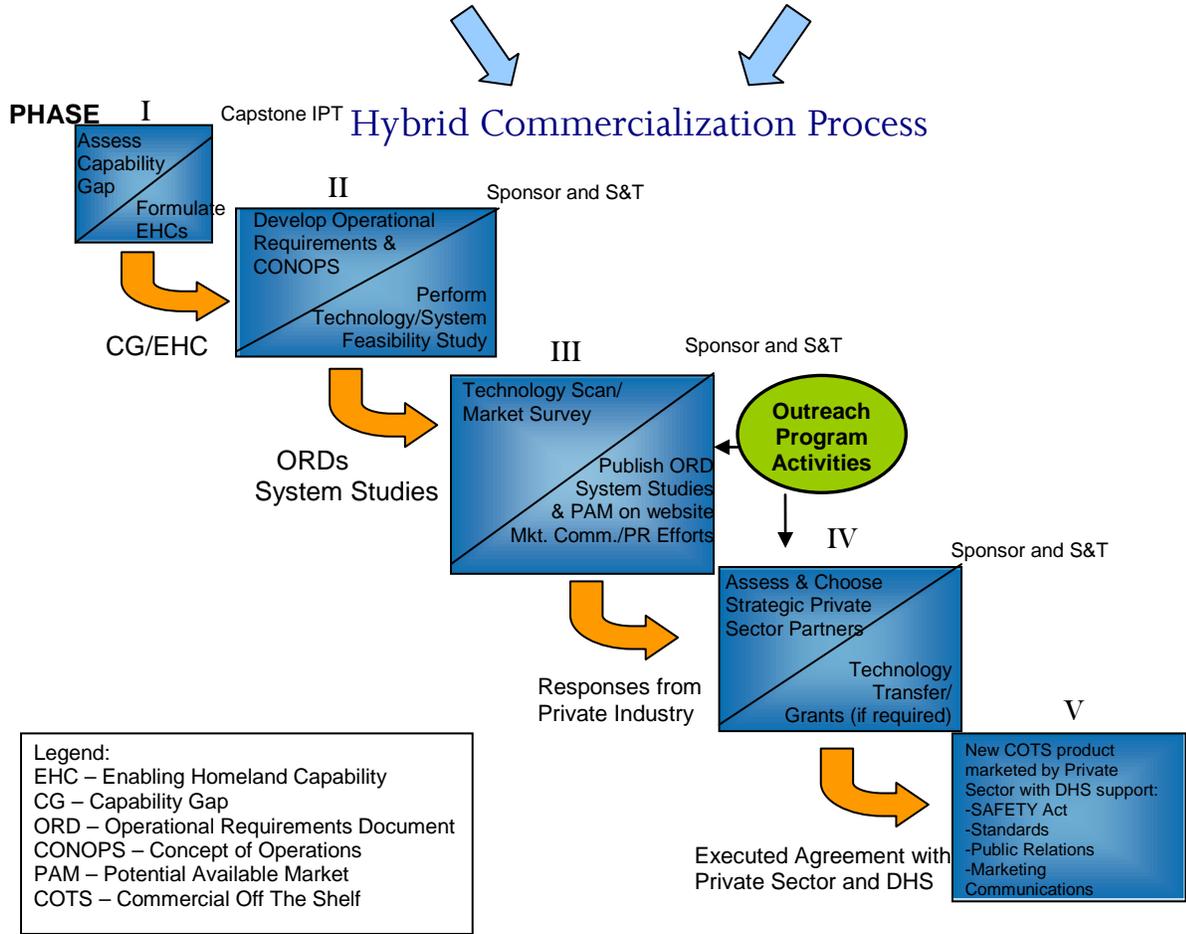
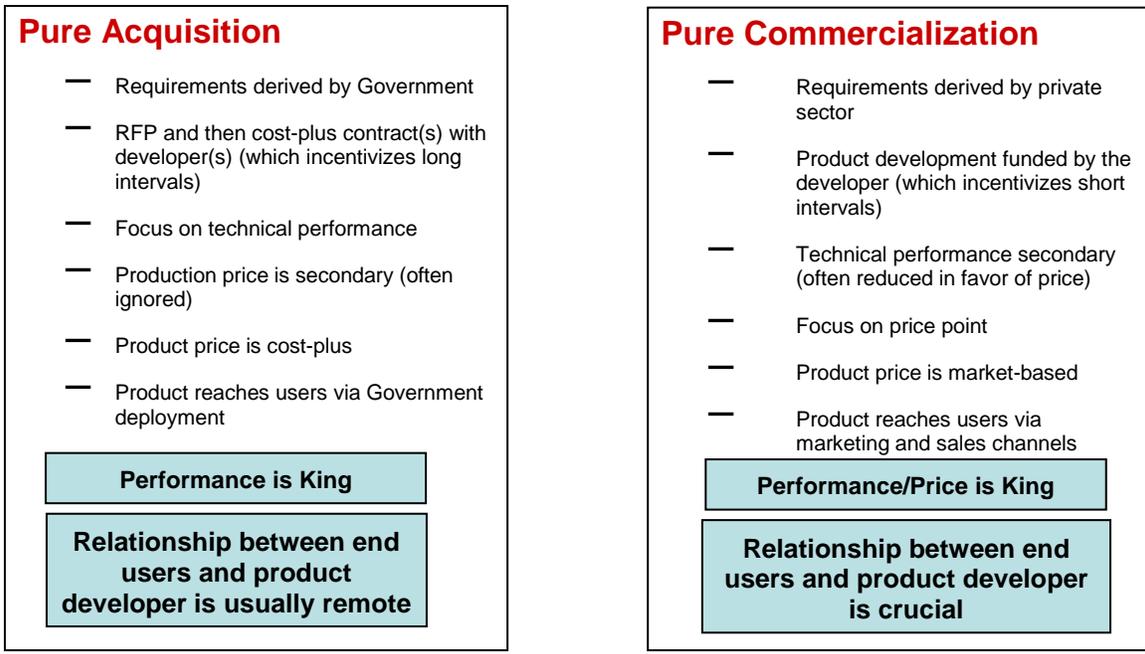


Figure 2: Comparison of “Pure Acquisition” versus “Pure Commercialization” models for product/system development and the resultant hybrid model implemented by DHS.

Figure 3 delineates the overall description of DHS' new commercialization model and its first private sector outreach program called the SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) Program to develop products and services in a private-public "win-win" partnership, recently approved in June 2008 by DHS and described in detail at www.dhs.gov/xres/programs/gc_1211996620526.shtm. Briefly, the SECURE Program is based on the premise that the private sector has shown that it is willing and able to use its own money, resources, expertise and commercialization experience to develop and produce fully developed products and services for DHS if significant market potential exists. The private sector has shown remarkable interest in devoting its time and money to such activities if and when an attractive business case can be made related to large revenue/profit opportunities that certainly exist at DHS and its ancillary markets to participate in the advancement of DHS commercialization efforts. The private sector requires two things from DHS: 1. detailed operational requirements, and 2. a conservative estimate of the potential available market(s). Once this information is posted to the SECURE Program website, small, medium and large companies are open to generate their own business cases and pursue possible participation in the program.

A New Model for Commercialization...

- Develop Operational Requirements Documents (ORDs)
- Assess addressable market(s)
- Publish ORD and market assessment on public DHS web portal, solicit interest from potential partners in a way that is open to small, medium and large businesses
- Execute no-cost (CRADA-like) agreement with multiple private sector entities and transfer technology and/or IP(if necessary)
- Develop supporting grants and standards as necessary
- Assess T&E findings after product is developed to assure DHS and ancillary markets that product meet its published specifications
- New Commercial-Off-The-Shelf (COTS) product marketed by private sector with DHS support

SECURE Program



- Application – Seeking products/technologies aligned with posted DHS requirements
- Selection – Products/Technologies TRL-5 or above, scored with internal DHS metrics
- Agreement – One-page streamlined CRADA document that outlines milestones and exit criteria
- Publication of Results – Recognized third-party T&E conducted on TRL-9 product/service. Results verified by DHS, posted on DHS web-portal to provide confidence to potential customers at DHS and its ancillary markets that product(s) meet or exceed their published specifications in reference to their actual performance.

Figure 3: Step-by-step guide to the commercialization process developed and adopted by DHS with a brief summary of the popular SECURE Program.

In order to provide DHS operating components, the first responder community and other end-users with products that meet their specific requirements, the SECURE program provides a vehicle by which private sector entities can offer products and/or conduct product development geared specifically toward meeting those needs. Private sector entities currently possessing a technology/product/system rated at a Technology Readiness Level TRL-5 (i.e. applied or advanced R&D) or above that potentially closes a defined DHS capability gap by addressing detailed operational requirements supplied by DHS-S&T on the SECURE Program website will have the opportunity enter into a CRADA-like agreement to continue development of their technology/product/system to TRL-9 (i.e. fully field deployable product) at their expense. The CRADA-like agreement also provides private sector entities with the assurance that DHS-S&T will verify their recognized independent third-party test(s) of a given technology/product/system. A Cooperative Research and Development Agreement (CRADA) is a written agreement between a private company and a government agency to work together on a project¹¹.

¹¹For more information on CRADAs, please visit: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+15USC3710a and <http://www.usgs.gov/tech-transfer/what-crada.html>.

Stage Four: Product Development

After DHS determines whether the Acquisition or the Commercialization process is appropriate, the fourth stage commences and the system prototype is demonstrated in an operational environment. S&T and the end user/customer have begun to develop a final transition plan and updates have been made to the operational and/or functional requirements document. Interoperability has been demonstrated and Management Directives (MD) have been reviewed to assure compliance. An operations and maintenance manual has been completed and a security manual has been developed.

Since the technology has been proven to work in its final form and under expected conditions, TRL 8 represents the end of true system development. Technology components are therefore form, fit, and function compatible with an operational system. The operational test report has been completed and a Limited User Test (LUT) Plan has been developed. A training plan has also been developed and implemented.

The actual system is then proven through successful mission operations and the end user fully demonstrates the technology in the CONOPS. All critical documentation has been completed and planning is underway for the integration of the next generation technology into the existing program components.

During the last stage, the private sector focuses on the manufacturing plan and the development effort includes the final design reviews, product prototypes along with documented product test results and other product development deliverables. Sales/Marketing update the marketing plan, the sales and distribution plan, and all sales materials. Manufacturing develops assembly and manufacturing procedures, designs and fabricates manufacturing tooling. Quality Assurance updates the Test Q/A plan and creates the quality plan. They also develop testing procedures, create test and fixture designs, perform reliability testing on the prototype and design and test the shipping container.

The goal of the private sector during the final stage is to demonstrate product manufacturing according to quality assurance standards while remaining within cost/schedule targets. The development effort concludes with a customer-adopted defect-free product, implemented engineering change orders and a final user's manual. Applications engineering and technical engineering support are then implemented. Sales/Marketing also provides sales training, creates a promotional plan and coordinates literature advertising and public relations. Manufacturing establishes the final manufacturing/assembly routines and procedures, the final manufacturing tooling, and the manufacturing document release and acceptance, then undertakes an analysis for future product cost reduction. Quality Assurance does the final QA and test pooling, prepares the final QA/test procedures, and compiles the manufacturing yield data.

Management reviews for both the public and private sector are required to ensure that the final exit criteria and deliverables are met. Since the actual system has been proven through successful mission operations, the product is then deployed to captive users or sold as COTS directly to end users.

Conclusion

The Commercialization Office has developed a number of processes, programs and tools to clearly articulate the needs of DHS. Outreach efforts are also critical and center on

notifying the private sector about opportunities that exist for partnership and business development to address the needs of the Department. Therefore, we have developed a “Product Realization Chart” that serves as a useful guide to relate and correlate terminology used by both the public and private sector in order to develop and deliver required technologies/products that meet the specific operational requirements of the Department of Homeland Security’s operating components and its end users such as first responders.



Thomas A. Cellucci, Ph.D., MBA is the U.S. Department of Homeland Security’s first Chief Commercialization Officer. In his role, he recently published two comprehensive guides: *Requirements Development Guide* and *Developing Operational Requirements* to aid in effective requirements development and communication for the department. He possesses extensive experience as a scientist and senior executive and Board Member in high-technology firms in the private sector.

Appendix E: DHS: Leading the Way to Help the Private Sector Help Itself (Article)

DHS: Leading the way to Help the Private Sector Help Itself

The Office of Infrastructure Protection offers a window into which the private sector can realize significant business opportunities

Thomas A. Cellucci, Ph.D., MBA
 Chief Commercialization Officer
 Commercialization Office
 U.S. Department of Homeland Security

Commercialization, broadly described as “the development of markets and the production and delivery of products/services to meet the unsatisfied needs/wants of these markets,” represents a key process that the U.S. Department of Homeland Security (DHS) now uses to generate product/services for its numerous stakeholders in a cost-effective and efficient way. DHS’s primary users of technology-based products are its seven operating components. However, DHS is also a conduit to numerous other users. For example, the Office of Infrastructure Protection (OIP) coordinates 18 Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs) organized under the National Infrastructure Protection Plan (NIPP). These SCCs represent various critical infrastructure and key resources (CIKR) owners and operators found in the chemical industry to power companies, for example. See Table 1 for the list of SCCs. Critical infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would create a debilitating effect on our security, national economic security, public health or safety, or any combination of the above. Key resources are publicly or privately controlled resources essential to the minimal operations of the economy and government.

Responsible Federal Agency	Sector Coordinating Council
U.S. Department of Agriculture	Agriculture and Food
Department of Health and Human Services	
Department of Defense	Defense Industrial Base
Department of Energy	Energy
Department of Health and Human Services	Public Health and Healthcare
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Water
DHS’s Office of Infrastructure Protection	Chemical Commercial Facilities Dams Emergency Services Nuclear Reactors, Materials, and Waste Critical Manufacturing
DHS’s Office of Cyber Security and Telecommunications	Information Technology Communications

DHS's Transportation Security Administration	Postal and Shipping
DHS's Transportation Security Administration, United States Coast Guard	Transportation Systems
DHS's Immigration and Customs Enforcement, Federal Protective Service	Government Facilities

Table 1 – HSPD-7 establishes a national policy for Federal departments and agencies to identify and prioritize critical infrastructure and to protect them from terrorist attacks.

Under Homeland Security Presidential Directive 7 (HSPD-7), Federal departments and agencies will identify, prioritize, and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them. Federal departments and agencies work with state and local governments and the private sector to accomplish this objective. The NIPP process provides clarity into the specific needs or requirements of the SCCs, which in turn generates information that yields rough estimates of the potential available markets (PAMs) for solutions that address a particular need.

The recently adopted, commercialization process allows DHS to develop and deliver products/services for the CIKR community in a more cost-effective and efficient manner as compared to a traditional governmental acquisition process; all at the benefit of the CIKR owners and operators in the private sector and, just as importantly, to the benefit of the American taxpayer. Through this commercialization process, DHS is fostering new and innovative partnerships with the private sector to cooperatively develop products/services aligned to the needs of the expansive CIKR market.

In a relatively short amount of time, DHS has developed, and is now implementing, a “commercialization mindset¹²” in its approach to responding to the needs of its valued stakeholders. The idea of utilizing a commercialization process at DHS is a much-needed and significant departure from the commonly employed acquisition model. Commercialization has the potential to yield significant benefits in terms of reducing federal R&D costs, enabling rapid time-to-market for newly developed commercial products/services for DHS and some of its other stakeholders like first responders and CIKR owners/operators. Rather than have DHS pay for the development of custom “one-off” systems, which are frequently required in many military applications, it is apparent that DHS has much to offer the private sector in terms of its large potential available markets requiring widely distributed products. Figure 1 shows the major differences between a “pure” acquisition versus a “pure” commercialization process, and our resultant DHS “hybrid” commercialization process. To put it simply, when widely-distributed products or services are required, commercialization should be utilized at the benefit of the taxpayer, DHS and the private sector.

¹² See, for example, *Developing Operational Requirements, Version 2, Product Realization Chart, DHS Implements a Commercialization Process* and other valuable resources online at http://www.dhs.gov/xres/programs/gc_1211996620526.shtm

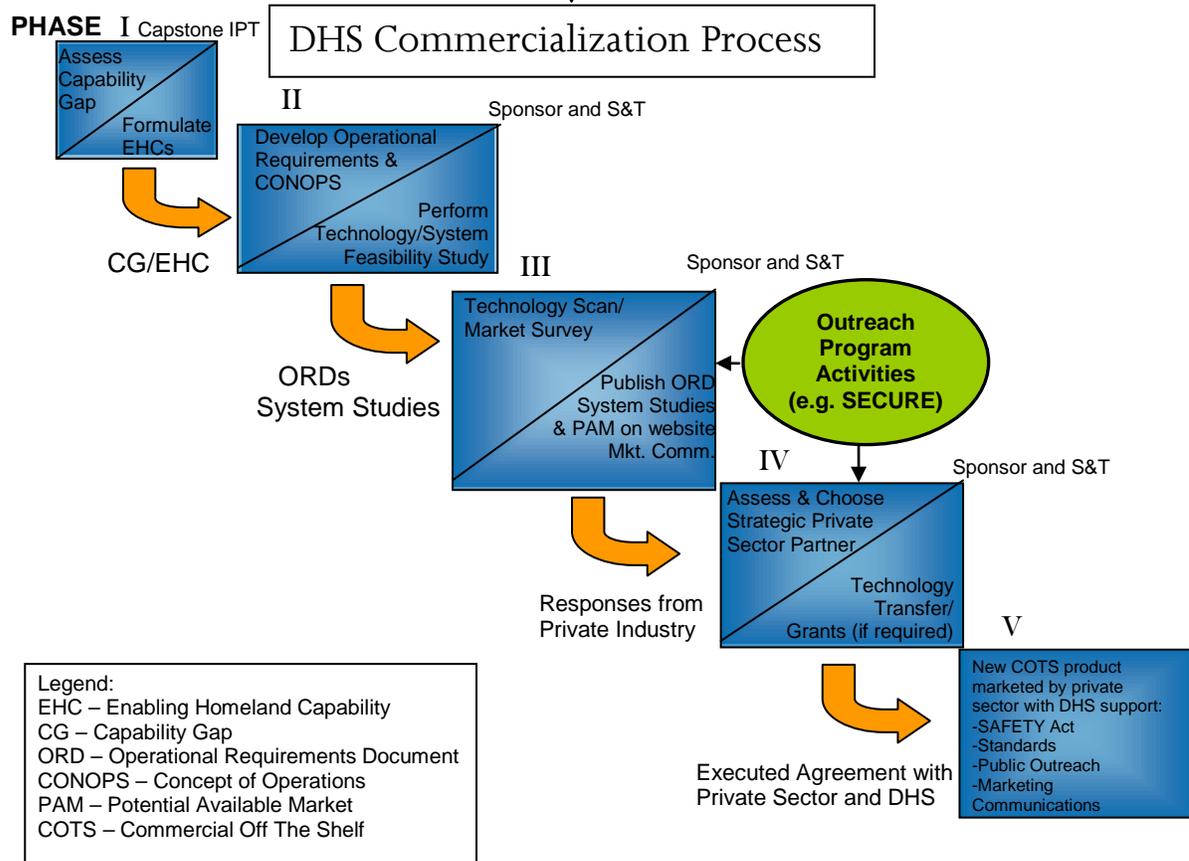
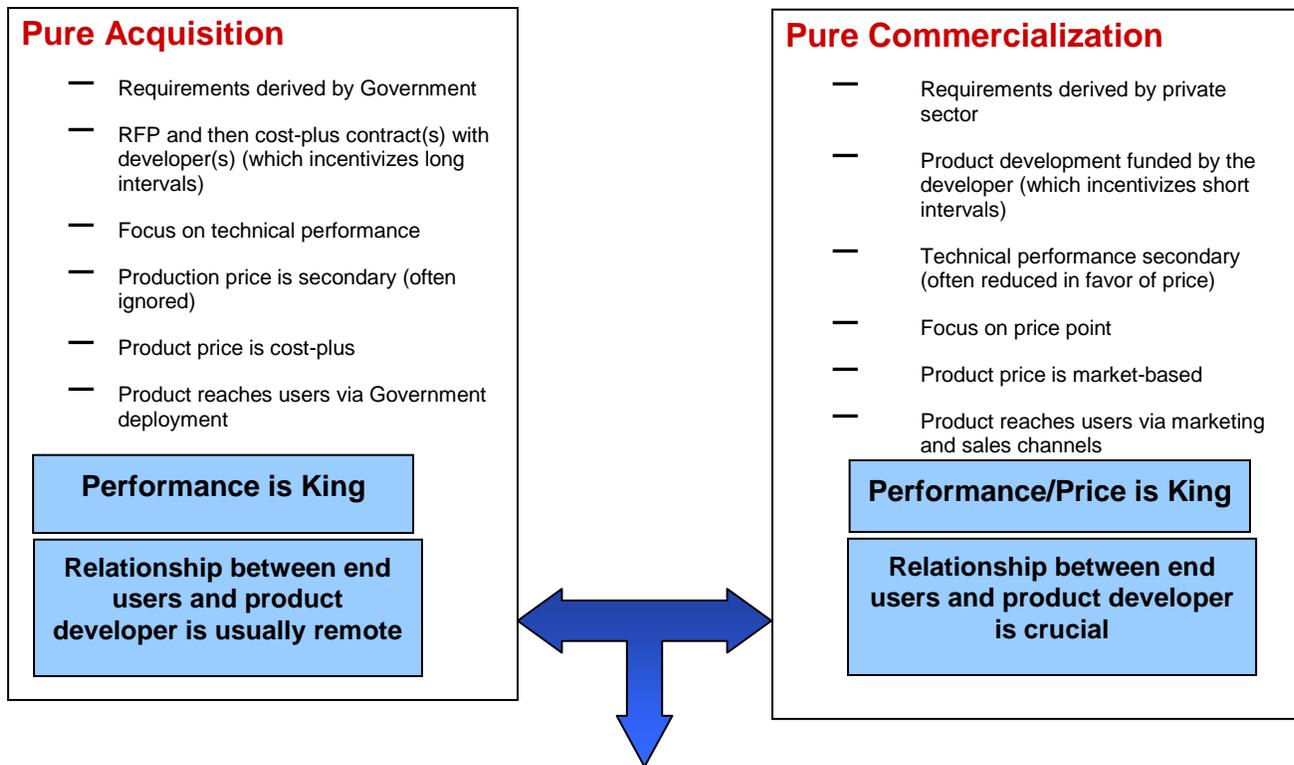


Figure 12 DHS’s commercialization process combines aspects of a “pure” Acquisition and commercialization model resulting in the current “hybrid” commercialization model.

The SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) Program, outlined in Figure 2, is an innovative public-private sector partnership effort leveraging the DHS commercialization process to meet end-user needs found at DHS, the first responder community and within the CIKR market. Briefly, the SECURE Program is based on the premise that the private sector has shown repeatedly that it is willing and able to use its own money, resources, expertise and experience to develop and produce fully developed products and services for DHS if significant market potential exists. The private sector has shown remarkable interest in devoting its time and money to such activities if and when an attractive business case can be made related to large revenue/profit opportunities, which certainly exist at DHS and its ancillary markets. The private sector requires two pieces of information from DHS: 1. detailed operational requirements, and 2. a conservative estimate of the potential available market(s) where a given product or service can be used. This information can then be verified by the private sector to generate a business case for their possible participation in the program.

SECURE Program

Overview of Concept of Operations



- **Application** – Seeking products/technologies aligned with posted DHS requirements
- **Selection** – Products/Services TRL-5 or above, scored with internal DHS metrics
- **Agreement** – One-page Cooperative Research and Development (CRADA)-like document that outlines milestones and exit criteria
- **Publication of Results** – Recognized Third-Party T&E conducted on TRL-9 product/service. Results verified by DHS, posted on DHS web-portal
Benefits:
 - ✓ Successful products/technologies share in the imprimatur of DHS
 - ✓ DHS operating components and first responders make informed decisions on products/services aligned to their stated requirements

Figure 13 A brief overview of the SECURE Program Concept of Operations. (See http://www.dhs.gov/xres/programs/gc_1211996620526.shtm)

While the development of highly specialized products is still relevant to the Department, DHS itself represents a substantial potential available market for widely distributed products; in many instances requiring thousands, if not millions of product or service units to address unsatisfied needs. Couple to this the fact that DHS has responsibility for an array of ancillary markets: namely, first responders and CIKR owners/operators, representing large potential available markets in their own right; it is evident that substantial business opportunities exist for the private sector. The NIPP process brings greater vision into the needs of the 18 SCCs previously described, which in turn generate the detailed operational requirements necessary for private sector efforts to

Given the fragmented nature of the CIKR communities, DHS, through the Science and Technology Directorate (S&T), created a crosscutting Capstone Integrated Product Team (IPT) to focus solely on the critical infrastructure protection needs and requirements of the CIKR communities. Figure 4 shows the general organization of a Capstone IPT along with the appropriate functions of each member. Our Infrastructure Protection IPT¹³ works closely with the Office of Infrastructure Protection to reach out to the various CIKR owners and operators across the country to gain valuable insight into their needs and requirements and provide a forum for them to be addressed.

S&T Transition IPT Members and Function

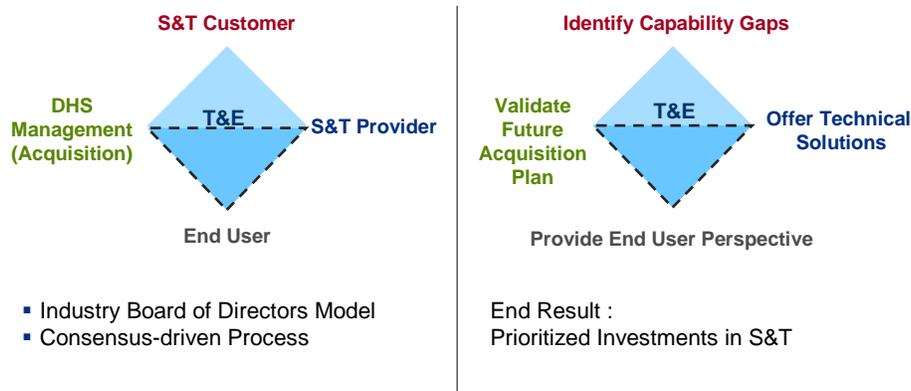


Figure 15 The Infrastructure Protection Capstone IPT will bring together end-users, scientists and program managers to discuss mission-critical capability gaps and requirements.

The Capstone IPT process ensures that quality, efficacious products and services are developed in close alignment with customer needs. Through a network of communication channels, Capstone IPTs bring together S&T division heads, management personnel and end-users (operating components, field agents and supporting first responders and/or CIKR owner/operators) involved in research, development, testing and evaluation (RDT&E). Working collaboratively, the Infrastructure Protection IPT collects, evaluates and prioritizes requirements to enable new mission-critical capabilities.

In providing critical information to the private sector in terms of the collection and articulation of detailed operational requirements and a conservative estimate of the potential available market, DHS has laid the foundation for cooperative product development with the private sector. These relationships drive the commercialization

¹³ Kikla, Richard V. and Cellucci, Thomas A. “Capstone IPTs: Even in Government the Customer Comes First,” April 2008.

process and ensure that end-users such as CIKR owners and operators receive needed products/services in a timely manner at minimal costs to DHS. Given these relationships, it is relatively easy to make a case for commercialization at the Department (see Figure 5) as it results in “wins” for the American taxpayer, public and private sectors.

Benefit Analysis – “Win-Win-Win”		
Taxpayers	Public Sector	Private Sector
1. Citizens are better protected by DHS personnel using mission critical products/services	1. Improved understanding and communication of needs	1. Save significant time and money on market and business development activities
2. Tax savings realized through private sector investment in DHS	2. Cost-effective and rapid product development process saves resources	2. Firms can genuinely contribute to the security of the Nation
3. Positive economic growth for American economy	3. Monies can be allocated to perform greater number of essential tasks	3. Successful products share in the “imprimatur of DHS”; providing assurance that products really work
4. Possible product “spin-offs” can aid other commercial markets	4. End users receive products aligned to specific needs	4. Significant business opportunities with sizeable DHS and DHS ancillary markets
5. Customers ultimately benefit from COTS produced within the Free Market System – more cost effective and efficient product development	5. End users can make informed purchasing decisions with tight budgets	5. Commercialization opportunities for small, medium and large business

Figure 16 A benefit analysis of the SECURE Program shows a number of positive outcomes for taxpayers as well as the public and private sectors.

In conclusion, our commercialization process is ideal in matching the detailed requirements of the collective CIKR community with product development efforts undertaken by the private sector who seek access to the large potential available markets. Commercialization is not only an attractive method by which DHS can develop products/services for CIKR owners and operators – but it is also beneficial to both the public and private sectors and – most importantly – to the American taxpayers at large.

Appendix F: SECURE™ Program (Article)

Partnership Program Benefits Taxpayers as well as Private and Public Sectors

SECURE™ Program enables the cost-effective and efficient development of products and services for Homeland Security.

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
Commercialization Office
U.S. Department of Homeland Security

A recently announced initiative at the U.S. Department of Homeland Security (DHS), called the SECURE™ (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) Program is part of an overall effort at the Department to create a “Commercialization Mindset” by leveraging the fact that while DHS has a limited budget compared to the Department of Defense, it does have something much more valuable – a large potential available market comprised of the seven DHS operating components (USCIS, TSA, FEMA, CBP, ICE, U.S. Coast Guard and U.S. Secret Service) and other large ancillary markets such as the diverse, yet substantial first responder market.

The SECURE Program is based on the premise that the private sector has shown that it is willing and able to use its own money, resources, expertise and experience to develop and produce fully developed products and services for DHS. When an attractive business case can be made related to large revenue/profit opportunities, which certainly exist at DHS and its ancillary markets. The private sector requires two vital pieces of information from DHS: 1. detailed operational requirements, and 2. a conservative estimate of the potential available market(s). This information can then be used to generate a business case for possible private sector participation in a program or project.

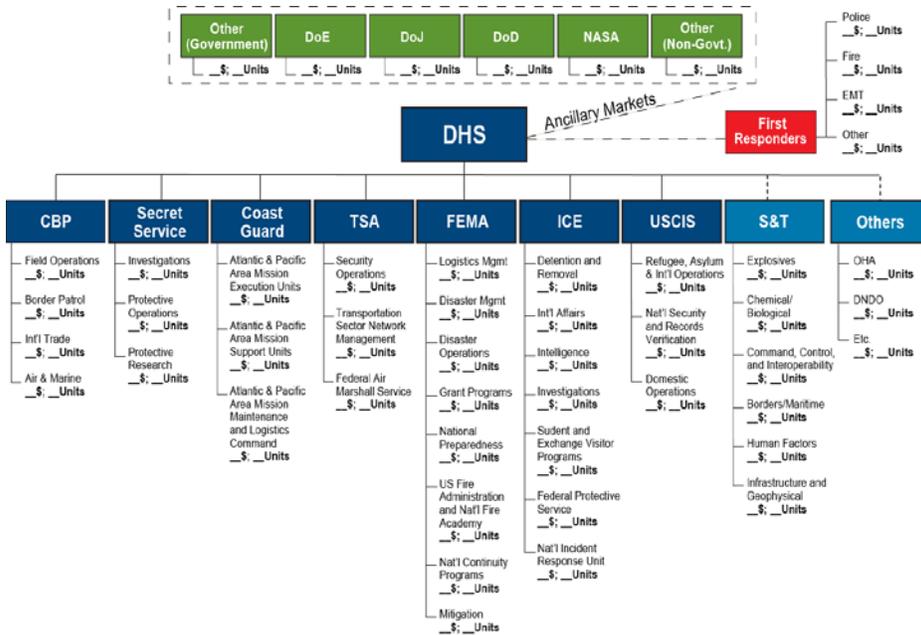


Figure 1: This Market Potential Template is used to estimate the given size of a particular market that DHS has identified as an area requiring new products or services.

This Market Potential Template is used to demonstrate how large (in both a dollar and unit volume perspective) a given market is for a particular product or service. Coupled with an Operational Requirements Document (ORD), the private sector receives ample information from DHS to generate a business case for developing a product or service sought after by DHS for its operating components or first responders, whose combined ranks are significant, as delineated in Figure 2.

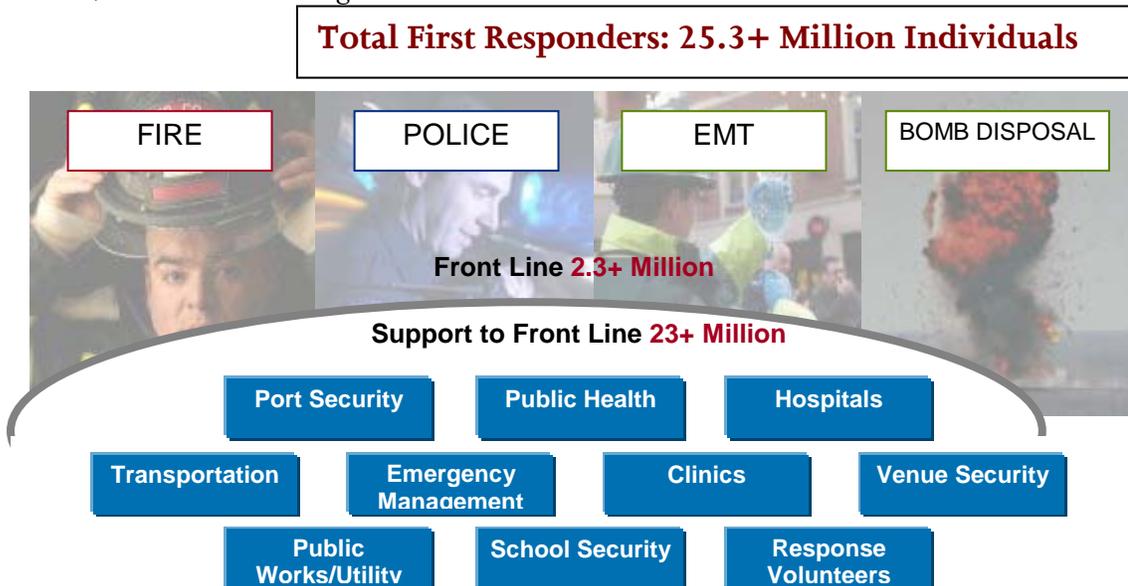


Figure 2: Homeland Security Presidential Directive Number 8 (HSPD-8) conservatively classifies 25.3+ million individuals as First Responders in the United States alone.

In return for providing this critical information, thus saving the private sector considerable time and money related to both market and business development activities, DHS expects the private sector to offer solutions – utilizing the free market system with open and fair competition – to meet published requirements. Simply stated, the private sector receives significant business opportunities, DHS and its supported entities, like the first responder communities, receive products and services developed at faster execution rates at the private sector’s cost – all to the benefit of the American taxpayer. See Figure 3 for an overview and benefits analysis of the SECURE Program.

SECURE Program Concept of Operations



- Application – Seeking products/technologies aligned with posted DHS/First Responder requirements
- Selection – Products/Technologies TRL-5 or above, scored with internal DHS metrics
- Agreement – One-page CRADA-like document that outlines milestones and exit criteria
- Publication of Results – Recognized Third-Party T&E conducted on TRL-9 product/service. Results verified by DHS, posted on DHS web-portal

SECURE Program Benefit Analysis – “Win-Win-Win”		
Taxpayers	Public Sector	Private Sector
1. Citizens are better protected by DHS personnel using mission critical products	1. Improved understanding and communication of needs	1. Save significant time and money on market and business development activities
2. Tax savings realized through private sector investment in DHS	2. Cost-effective and rapid product development process saves resources	2. Firms can genuinely contribute to the security of the Nation
3. Positive economic growth for American economy	3. Monies can be allocated to perform greater number of essential tasks	3. Successful products share in the “imprimatur of DHS”; providing assurance that products really work.
4. Possible product “spin-offs” can aid other commercial markets	4. End users receive products aligned to specific needs	4. Significant business opportunities with sizeable DHS and DHS ancillary markets
5. Customers ultimately benefit from COTS produced within the Free Market System – more cost effective and efficient	5. End users can make informed purchasing decisions with tight budgets	5. Commercialization opportunities for small, medium and large business

product development		
---------------------	--	--

Figure 3: Brief overview of the SECURE Program' Concept-of-Operations and a benefits analysis.

To learn more about the SECURE Program and other opportunities for the private sector, please visit http://www.dhs.gov/xres/programs/gc_1211996620526.shtm or contact the Commercialization Office at SandT_Commercialization@hq.dhs.gov.

Appendix G: FutureTECH™ Program

FutureTECH™: Guidance to Understanding Future DHS S&T Critical Research/Innovation Focus Areas

New program in the Commercialization Office enables the private sector and others to peer into critical research/innovation focus areas of interest to the DHS Science and Technology (S&T) Directorate.

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
Commercialization Office
U.S. Department of Homeland Security

Due to the popularity of the SECURE™ Program introduced by the recently formed Commercialization Office, the U.S. Department of Homeland Security (DHS) Science and Technology (S&T) Directorate has now introduced a “sister program” called FutureTECH. The SECURE Program leverages the experience and resources of the private sector to develop fully deployable [i.e., technology readiness level nine, (TRL-9)] products and/or services based on DHS generated and vetted detailed operational requirements documents (ORDs) and a conservative estimate of the potential available market (represented by DHS operating components and ancillary markets comprised of first responders, critical infrastructure/key resources (CI/KR) owners/operators and other DHS stakeholders). The FutureTECH™ Program, on the other hand, is reserved for those critical research/innovation focus areas that could be inserted eventually into DHS acquisition or commercialization programs when development reaches TRL-6 based on metrics and milestones more specific than those of a broad technology need statement alone, yet not as specific as a detailed ORD.

FutureTECH identifies and focuses on the future needs of the Department as fully deployable technologies and capabilities, in many cases, are not readily available in the private sector or Federal government space. While the SECURE Program is valuable to all DHS operating components, organizational elements and DHS stakeholders, FutureTECH is intended for DHS S&T use only, particularly in the fields/portfolios related to Research and Innovation (see for example, http://www.dhs.gov/xabout/structure/editorial_0531.shtm for details on research and innovation activities and programs).

DHS S&T Basic Research Portfolio

The DHS S&T Basic Research Portfolio creates fundamental knowledge for enhancing homeland security, normally at a time frame exceeding 8 years. These efforts emphasize (but are not limited to) university fundamental research and governmental lab discovery and invention. Basic Research programs are executed in the Directorate’s six divisions, facilitated by the Office of National Laboratories and the Office of University Programs and are closely coordinated with other government agencies.

Typically, the basic research efforts at S&T are motivated by one or more of the following:

1. The research addresses an important DHS issue (such as a High-Priority Technology Need) without a viable near-term solution.

2. The research pursues a creative solution that addresses a unique, long-term DHS need that is not addressed elsewhere.
3. The research exploits new scientific breakthroughs (e.g., from universities, laboratories, or industry) that could strengthen homeland security.

The Research Leads in S&T’s six divisions developed Basic Research focus areas that represent the technological areas in which S&T seeks to create and/or exploit new scientific breakthroughs. These focus areas, generated with input from the research community and vetted through S&T’s Research Council, will help guide the direction of the S&T Basic Research Portfolio, within resource constraints, to provide long-term science and technology advances for the benefit of homeland security.

DHS S&T Innovation Portfolio

The DHS S&T Innovation Portfolio focuses on homeland security research and development (R&D) that could lead to significant technology breakthroughs that could greatly enhance DHS operations.

The Office of the Director of Innovation oversees S&T’s Homeland Security Advanced Research Projects Agency (HSARPA). Established by the Homeland Security Act of 2002 (P.L. 107-296), HSARPA funds R&D of homeland security technologies to “support basic and applied homeland security research to promote revolutionary changes in technologies that would promote homeland security; advance the development, testing and evaluation, and deployment of critical homeland security technologies; and accelerate the prototyping and deployment of technologies that would address homeland security vulnerabilities.”

Innovation/HSARPA personnel work closely with the Under Secretary for Science and Technology, S&T divisions, DHS components, industry, academia, and other government organizations to determine topic areas for projects. Innovation’s efforts are complementary to S&T’s other programs and projects, pushing scientific limits to address gaps in areas where current technologies and R&D are inadequate or non-existent. Please see Table 1 for a current delineation of Innovation project areas.

Table 1: Description of Innovation Project Areas Categorized as High Impact Technology Solutions (HITS) and High Innovative Prototypical Solutions (HIPS) Projects.

High Impact Technology Solutions (HITS) Projects	
Cell-All Ubiquitous Chem/Bio Detect	Examines proofs-of-concept for integrating miniaturized chemical and biological agent detectors into personal devices, such as cellular telephones, in order to create a widely distributed network for detection, classification and notification in the event of a chemical release, and with possible extensions to detect chemical components of some biological agents. Individual device owners on the network would control the detection and transmission of the data, sensor timing and global positioning satellite (GPS) location information. The goals of this project include significant improvement to chemical and biological detectors’ integration, size, costs, power, maintenance, durability and response characteristics.
Wide Areas Surveillance	Focuses on surveillance and tracking in densely populated infrastructure settings and urban landscapes (such as airports, train stations, city streets and squares) to protect the nation’s highest priority infrastructure. In FY 2008, the project constructed an array of multiple

	<p>high-resolution cameras that are digitally integrated into a single view with an overall resolution of 100 mega pixels. The system provides high-resolution imagery and allows multiple operators to simultaneously view and manipulate (e.g., zoom and scan) regions of the scene in high-resolution detail while maintaining a full 360-degree field of view. The system includes automated change detection capabilities, and users can rapidly scan video images for forensic analysis. In FY 2009, the project plans to conduct a demonstration to evaluate the effectiveness of the system in a densely populated environment and also significantly advance the system hardware to more than double the current resolution and ultimately improve system cost effectiveness.</p>
Resilient Tunnel Project	<p>The project focuses on designing an inflatable tunnel plug to protect mass transit tunnels from fires, smoke and flooding. In FY 2008, the project initiated a partnership with the Washington Metropolitan Area Transit Authority (WMATA) and conducted a demonstration in a WMATA subway tunnel in August 2008. The results illustrated that a full-scale plug can be inflated quickly and efficiently in a real-world transit environment and that the plug effectively seals against the tunnel walls. In FY 2009, the project plans to conduct numerical modeling to optimize plug structure and performance; construct new small-scale plugs with stronger materials and optimized geometries; and subject these plugs to pressurized testing in the laboratory to simulate tunnel flooding.</p>
Tunnel Detect Project	<p>Develops detection technologies to locate clandestine underground tunnels that are used for cross-border illegal activities such as smuggling. In FY 2008, the project conducted a series of demonstrations of an electromagnetic gradiometer (radio frequency) mounted on an unmanned aircraft system, which is planned for further evaluation by Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) in FY 2009. Research and development activities include incorporating other sensors such as a hyper-spectral camera that detects differences in the environmental characteristics (e.g., moisture) at or near the tunnels that are indicators of the presence of a tunnel. The project initiated a parallel effort to prototype and test advanced ground-penetrating radar for tunnel detection. In FY 2009, S&T will test and demonstrate an advanced ground-penetrating radar and investigate additional technologies by leveraging Department of Defense (DOD) tunnel-detection efforts for border protection applications.</p>
Homeland Innovative Prototypical Solutions (HIPS) Projects	
Future Attribute Screening Technologies Mobile Module (FASTM2) (formerly Future Attribute Screening Technologies) Project	<p>Develops real-time, mobile screening technologies to automatically and remotely detect behavior indicative of intent to cause harm (identified as malintent) at screening checkpoints. In FY 2008, the project identified potential behavioral (illustrative gestures, gait, blinking, eye-gaze, etc.), physiological (change in heart beat, respiration, thermal, etc.), and paralinguistic cues that are likely indicative of malintent and identified remote sensors capable of detecting the associated physiological signals. The feedback from initial peer review and independent, nationally recognized subject matter experts was positive.</p> <p>In FY 2008, the project demonstrated the FAST laboratory module which is a functional test laboratory for the development, integration and implementation of real-time, mobile screening and future sensing technologies. In FY 2009, the project will continue validating and updating the malintent theory, sensors, and the module environment and incorporate the initial elements of data fusion and machine learning to improve screening accuracy. Independent peer review will be an ongoing element of the project to promote objectivity and ensure all aspects of the project are addressed. In FY 2009, the project will conduct an operational demonstration of a real-time intent detection capability.</p>
Hurricane & Storm Surge Mitigation Project	<p>Develops methods to better understand and accurately predict the behavior of a hurricane to help better predict its future track and to reduce the intensity and/or duration of a hurricane or storm. The focus will be on understanding the dynamics of storms as they grow from depressions to full hurricanes, and to try to determine if any of the dynamic variables can be used or manipulated against the storm itself in order to prevent further growth in strength. State and local officials will be able to more accurately and quickly</p>

	<p>determine which areas to evacuate. This project will focus on discovering variables to affect that could reduce the intensity and/or duration of a hurricane or storm before the storm reaches a point of runaway growth in strength. This project, in partnership with the National Oceanic and Atmospheric Administration (NOAA), will apply knowledge gained in the last 25 years (since the last attempt to modify hurricanes) to understand and model the life-cycle of a hurricane and identify/evaluate the effects of salt seeding, carbon black aerosol, upper ocean cooling, ion generators and monolayer films. The goal is not to stop hurricanes, which are an important part of the natural cycle, but to mitigate damage to life and property.</p>
<p>Levee Strengthening & Damage Mitigation Project</p>	<p>Develops techniques to rapidly repair breaches. Innovation has been able to work with S&T's Infrastructure and Geophysical Division to demonstrate technology for rapid repair.</p> <p>In September of FY 2008, the project successfully demonstrated technologies for rapid repair of levee breaches at the United States Department of Agriculture (USDA) facilities in Stillwater, Oklahoma. This proof-of-concept attracted the attention of potential end users and will lead to the development of full-scale systems. In FY 2009, the project will further develop the rapid repair prototypes for a full-scale demonstration and develop a concept of operations.</p>
<p>Resilient Electric Grid (REG) Project</p>	<p>Demonstrates Inherently Fault Current Limiting High-Temperature Superconducting (IFCL-HTS) technologies for reliable distribution and protection of electrical power. This technology would save millions-to-billions of dollars by providing continuous power in the event of a terrorist attack, brown outs, or black outs, and provide more efficient power distribution in the course of normal day-to-day operations.</p> <p>In FY 2008, the project conducted proof-of-concept demonstrations of a 3-meter, IFCL-HTS cable. The first demonstration in December 2007 showed that an HTS cable could transmit power with no electrical losses and simultaneously prevent cascading failures under normal conditions (i.e., no current overloads). Subsequently, the February 2008 demonstration was an important Go/No-go decision point because it confirmed that the HTS cable provides significant fault current limiting and also identified potential challenges due to higher than expected Alternating Current (AC) losses in the HTS cable. The project team conducted additional experiments and demonstrations in May 2008 to isolate the causes of the higher than expected AC losses and a third 3-meter cable was tested in August 2008. The results justified going forward with a 25-meter demonstration in FY 2009 at Oak Ridge National Laboratory. The project team successfully demonstrated the fault current limiting capability of the 25 meter test cable in March 2009. The project is planning an in-grid demonstration of the IFCL-HTS cable in the Manhattan grid for evaluation under operational conditions.</p>
<p>Safe Container (SAFECON) Project –</p>	<p>Investigates various technologies, including probe systems that detect and identify dangerous cargo and could be mounted on cranes used for on- and off-loading ship-carried containers. SAFECON also looks for sensors and specialized container materials designed to make screening more effective. The project aims to provide the capability to scan containers entering the country while minimizing the impacts to commerce; high reliability, high-throughput detection of weapons of mass destruction (WMD), explosives, contraband and human cargo; and immediate detection and isolation of suspected threat containers.</p> <p>In FY 2008, the project completed threat characterization and container characterization studies at the ports of Charleston, South Carolina and Boston, Massachusetts to inform decisions on sensor and prototype development. SAFECON also began the development of a remote vapor inspection system using advanced laser techniques to detect and identify threat chemicals and explosives. In FY 2009, the project will demonstrate</p>

	<p>integrated chemical and explosives sensor performance in a laboratory.</p> <p>In addition to the approach described above for rapid detection while the container is being moved by crane, DHS S&T is also looking at an alternative approach that takes advantage of the long transit time most shipping containers experience as they transit from their port of origin to the United States. This part of the SAFECON program is called Time Recorded Ubiquitous Sensor Technology (TRUST). It would allow detection of Chemical, Biological, Radiological, Nuclear, Explosive and personnel (CBRNE/P) threats within any container while in its port of embarkation or in transit, thus enabling authorities to route a suspect container to a safe location for special handling and an entry determination prior to entering a U.S. port.</p>
<p>Scalable Common Operational Picture Experiment (SCOPE) Project</p>	<p>Leverages an existing effort by DOD. The DOD effort, called the Joint Concept Technology Demonstration for Global Observer, is developing a high-altitude, long-endurance unmanned aircraft system (GO UAS). This aircraft-mounted system will enable homeland security personnel at the federal, state and local levels to collectively see what is happening during an event and potentially provide a communication platform for regions where infrastructure has been destroyed. This will allow responders to quickly understand the extent of a natural disaster or terrorist attack, enable communications and provide sufficient time to make critical decisions and mount a coordinated response. Today, no such capability exists.</p> <p>In FY 2008, the project developed and integrated modular sensor and communication payloads and began the formal GO Critical Design Review (CDR). In early FY 2009, the project successfully completed CDR and will conduct a series of operational utility assessments that will serve as a proof-of-concept for DHS operational security needs.</p>
<p>Rapid Liquid Component Detector (MagViz) Project</p>	<p>Uses ultra-low-field Magnetic Resonance Imaging (MRI) technology to screen baggage for liquid explosives. To mitigate the liquid explosives threat, airline passengers currently must pack liquids or gels (such as certain toiletries and medicines) in containers that are 3 ounces or smaller. Those containers must be placed in a 1-quart-sized, clear plastic, zip-top bag; and only 1-bag-per-traveller is allowed. These are known as “3-1-1 bags,” which undergo an X-ray inspection and possibly secondary screening using multiple methods, such as visual inspection. The goal of MagViz is to eliminate the 3-1-1 rule and allow passengers to place liquids in their carry-on baggage. MagViz will scan and identify individual materials that may be packaged together or separately as they go through the scanning process and evaluate them against a database that will differentiate between those items considered safe for carrying onto an aircraft (e.g., benign liquids and gels like mouthwash, toothpaste, etc.) and harmful ones. The intent is for the detection of liquids in baggage to be non-contact and to occur at the same rate as current X-ray machines, thus not hindering passenger throughput.</p> <p>In FY 2008, the project built and demonstrated a 3-1-1 bag-screening prototype in a lab. The August 2008 laboratory demonstration of this system showed that it can recognize and compare a wider range of liquids to a stored database and discriminate between harmful and benign liquids and gels with greater sensitivity and discrimination capability than previous demonstrations by overcoming operational challenges such as the orientation of containers and containers within containers.</p> <p>In December 2008, the project conducted a full demonstration of the 3-1-1 bag-screening prototype in an airport to assess its ability to detect liquid explosives within baggage in an operational setting. This public demonstration successfully showed that the prototype could distinguish between liquids in an operational environment overcoming challenges that could affect its sensitivity. Also in FY 2009, the project will build an exhaustive database of liquids through magnetic characterization and further address clutter in the operational environment; evaluate the capability of MagViz to detect dangerous solids; and demonstrate the capability of its research prototype to inspect at a depth of 20 cm. In FY 2010, the project plans to continue building the magnetic characterization database of liquids and demonstrate the capability of MagViz to seamlessly screen segregated liquids</p>

(without the 3-1-1 bag constraint) in an operational environment and subsequently evaluate termination or transition options.

DHS S&T Transition Portfolio

The DHS S&T Transition Portfolio focuses on the identification, evaluation and management of the near-term technology portfolio to develop and deliver advanced capabilities to DHS operating components, stakeholders and end-users for homeland security improvements. The Capstone Integrated Product Team (IPT) process is the framework that determines that developed capabilities meet operational needs, analyzes gaps in strategic needs and capabilities, determines operational requirements, and develops programs and projects to close capability gaps and expand mission competencies. This process is a DHS customer-led forum through which the identification of functional capability gaps and the prioritization of these gaps across the Department are formalized. The IPTs oversee the research and development efforts of DHS S&T and enable the proper allocation of resources to the highest priority needs established by the DHS operating components and first responders.

FutureTECH Program

Scope:

This program enables DHS S&T to efficiently and cost-effectively leverage the resources, skills, experience and productivity of the private sector and other non-DHS entities to develop technologies/capabilities in alignment with research/innovation focus areas obtained from DHS S&T (see above for examples). These technologies/capabilities, when successfully developed, may ultimately be used by DHS, the first responder community, critical infrastructure/key resources (CI/KR) owners/operators and other DHS stakeholders. In essence, FutureTECH provides a "window of visibility" or "preview" of research/innovation focus areas that DHS and its stakeholders believe are essential in future products and services where detailed operational requirements documents (ORDs) can not be fully developed at this time. The program also provides insight into areas where Independent Research and Development (IRAD) monies could be spent by firms possessing funding to address DHS research/innovation focus areas.

Analogous to the popular SECURE Program, FutureTECH is another innovative private-public partnership and outreach program that outlines focus areas for which current technology only exists at earlier stages on the technology readiness scale (TRL 1-6). Technologies developed in alignment to stated focus areas could lead to cost-effective and efficient product development (TRL 7-9) when detailed requirements contained in ORDs are available. Like the SECURE Program, DHS will provide information to the public in an open and free way. The private sector and other non-DHS entities may use their own resources (including IRAD) to develop technologies/capabilities that will be of potential benefit to the DHS mission. Like the SECURE Program, DHS may enter into a simple CRADA (Cooperative Research and Development Agreement) document with an organization that shows it has the ability to deliver technology aligned with the research/innovation focus area sought after by DHS.

To state it simply, the SECURE Program focuses on product/service development to create products and services to protect our nation in the shorter term, while FutureTECH focuses on science and technology development related to critical research/innovation

focus areas. Like all of the Commercialization Office's programs, all parties "win" in the FutureTECH Program--the private sector and other non-DHS entities by receiving valuable insight into future research/innovation focus areas needed by DHS and its stakeholders. DHS "wins" because it will leverage the valuable skills, experience and resources of the private sector and others to expedite efficient and cost-effective technology development; the non-DHS entities "win" because they receive valuable information useful for their own strategic plans; and most importantly, all American taxpayers "win" because this innovative partnership yields valuable technologies/capabilities aligned with research/innovation focus areas developed in a more cost-effective and efficient way saving taxpayer money.

Overall Process:

Figure 1 is a graphical representation of the overall outreach process the Commercialization Office continues to implement to stimulate and engage the private sector and other non-DHS entities to use their resources to rapidly develop technology aligned with research/innovation focus areas that can yield significant benefits for DHS S&T with a speed-of-execution not typically observed in the public sector.

Outreach to the Private Sector

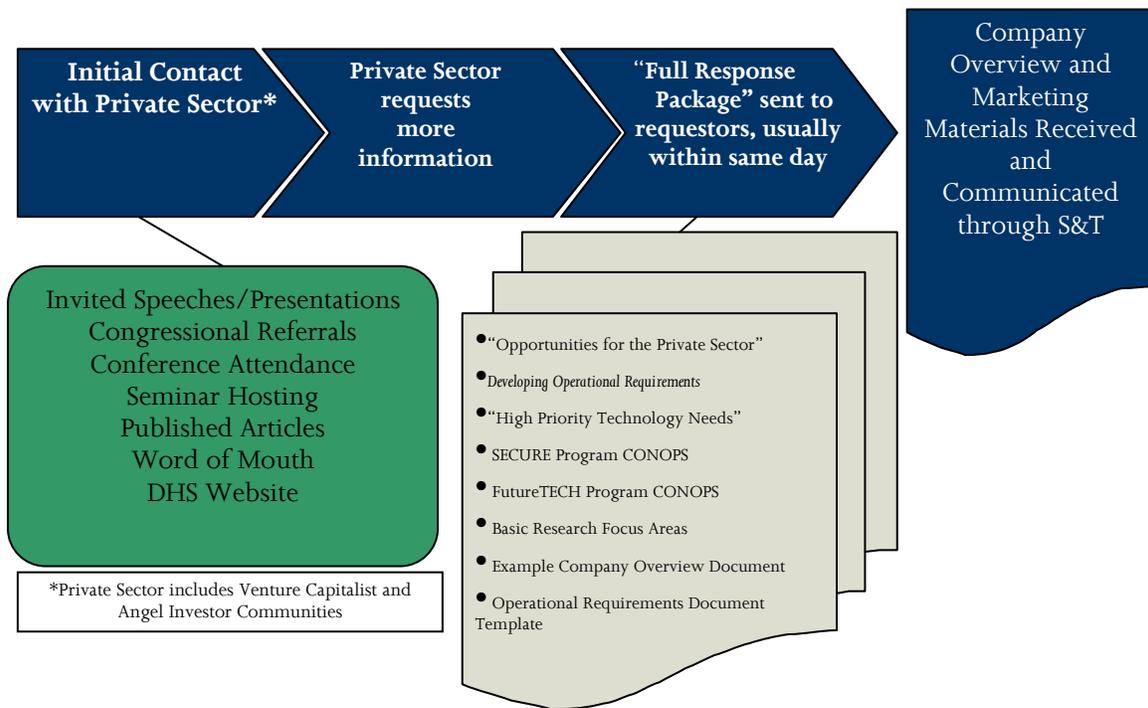


Figure 1: Overview of S&T Directorate Private Sector Outreach Process

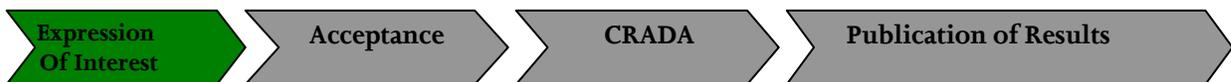


Program Process:

DHS S&T will provide this FutureTECH vehicle by which the private sector and other non-DHS entities can identify or develop technology aligned with research/innovation focus areas ranging from TRL-1 through TRL-6 (not fully developed TRL-9 products and/or services) based on DHS S&T's insight and knowledge mainly through its Research and Innovation portfolios/areas.

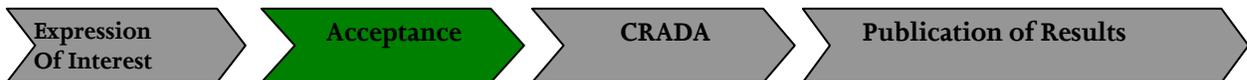
This approach enables DHS S&T to collaborate on the development of technology aligned with several research/innovation focus areas in an open and free way. The private sector and other non-DHS entities receive information on what new technologies will be required over-the-horizon to protect our nation, removing much of the “guess work” normally associated with predicting future needs.

As with the popular SECURE Program, DHS will review third party, recognized test and evaluation data to ensure that all milestones/objectives of an executed CRADA agreement are met and DHS will place a given research/innovation focus area solution developed by an entity on the FutureTECH website demonstrating that the research/innovation focus area has met DHS's broadly defined requirements (in contrast to the SECURE Program where products or services must demonstrate compliance to detailed operational requirements contained in an ORD).



Expression of Interest:

In the adherence to fairness of opportunity, and in order to capitalize on the free-market system, DHS S&T intends to publish this program and all ancillary requirements documents/information on the DHS website. These materials will be accessible by ALL. Given this information, the private sector and other non-DHS entities may contact DHS S&T if they are interested in developing or enhancing their technology within a research/innovation focus area in cooperation with DHS S&T. Potential research/innovation focus areas for this program (along with a simple CRADA agreement used in the SECURE Program) are provided on our website. The private sector organization or non-DHS entity must provide DHS S&T with basic, non-proprietary business information, contact information and demonstrate their potential alignment to widely available DHS S&T research/innovation requirements that are more detailed than what are commonly referred to as technology need statements, yet not as detailed as a well-defined ORD.



Acceptance:

In order to be fully considered by DHS S&T for cooperative research/innovation focus area technology development:

An entity must demonstrate they either possess technology at TRL-1 or higher (i.e. basic research) or possess the ability to develop a technology aligned with the research/innovation focus area to TRL-6 for later technology insertion into a potential acquisition or commercialization program.

The private sector and other non-DHS entities must propose a research/innovation focus area technology development effort that has clear and substantial alignment with any published DHS S&T requirements delineated above.

A DHS committee will be established to review the private sector and/or non-DHS entities' potential alignment to DHS research/innovation focus areas, and monitor the mutually-agreed-upon roles and responsibilities of partnership participants. The committee will consider these and other DHS proprietary metrics for determining which opportunities to pursue.



CRADA:

The private sector and/or non-DHS entity and DHS S&T could execute a simple, straightforward and binding CRADA whereby the non-DHS entity details milestones with dates and, in most cases, agrees to bear full and total financial responsibility to develop its technology aligned within the research/innovation focus area to a TRL-6 state. Under the Stevenson-Wydler Act (which is the statutory authority enabling DHS to enter into CRADAs), agencies may not contribute funds under a CRADA; however, they may contribute know-how, expertise, materials and equipment. It is important to mention that the execution of a CRADA agreement is at the sole discretion of the corresponding DHS S&T program manager. Additionally, a CRADA with DHS S&T will not necessarily lead to any follow-on contract actions or solicitations by DHS or other government agencies. Any solicitations for funding agreements related to technology areas collaborated upon in a CRADA would be subject to full and open competition. DHS S&T will publish on the DHS S&T website the factual finding(s) of any final assessment. DHS S&T has the right to cancel an agreement if the non-DHS entity does not fulfill/achieve its milestones or performance objectives by the mutually-agreed-upon dates.



Publication of Results:

It is apparent that the private sector and other non-DHS entities highly value DHS S&T's potential assessment of a given technology's recognized third-party test and evaluation (T&E) data. DHS S&T will openly publish summary findings and an acknowledgement of an entity's attainment of performance objectives on the DHS public web portal for review by the DHS operating components, first responder communities, CI/KR owners/operators and other potential users.

Acknowledgement

Many individuals contributed to the development of this article and the new FutureTECH Program, primarily the scientists, engineers, program managers and others within the S&T Directorate. Special thanks to the Research Leads within the divisions and the rest of the Research Council for development of the Basic Research focus areas. Ryan Policay is also thanked for his substantial contributions to this worthy effort.



Thomas A. Cellucci, Ph.D., MBA is the U.S. Department of Homeland Security's first Chief Commercialization Officer. In his role, he recently published four comprehensive books: *Requirements Development Guide*, *Developing Operational Requirements*, *Developing Operational Requirements (Version 2.0)* and *Harnessing the Valuable Experience and Resources of the Private Sector for the Public Good: DHS's Entry into Commercialization* to aid in effective requirements development and communication for the Department. He possesses extensive experience as a senior executive and Board Member in high-technology firms in the private sector. He is also the first federal official on the Council of Competitiveness representing the U.S. Department of Homeland Security.

Appendix H: Focus on Small Business

Focus on Small Business

Opportunities abound for “Engines of Innovation”

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
Commercialization Office
U.S. Department of Homeland Security

The Commercialization Office prides itself with the attention it pays to small businesses of all kinds – including minority-owned, HUB Zone, veteran-owned and other disadvantaged business. It is well known that much of our nation’s (and the world’s) innovation emanates from small business, but they often find some of their most difficult challenges with raising capital or performing effective market research necessary for business growth. To address these challenges, we have visited and met with thousands of small business owners, CEOs and entrepreneurs/innovators across the United States to inform them of the business opportunities that exist at the U.S. Department of Homeland Security (DHS). In addition, we have developed a series of books recently published by DHS that small businesses can use to augment and enhance their ability to efficiently and cost-effectively develop market-driven products and/or services. We have also produced numerous well-received articles and materials germane to small business. Refer to http://www.dhs.gov/xres/programs/gc_1234200779149.shtm for more detailed information and access to all of these useful resources.

The Commercialization Office continues to travel extensively throughout the United States to meet with small business through our Science and Technology (S&T) Directorate private sector outreach efforts. Statistical information on these efforts is posted to our website and updated on a quarterly basis. It is also important to note that DHS has a number of valuable resources small business may explore. The following are handy references for small business:

U.S. Department of Homeland Security and other Federal Contact Information:

DHS and/or Federal Contact	Description	Contact Information
Private Sector Office	Part of the DHS Office of Policy, the Private Sector Office engages individual businesses, trade associations and other non-governmental organizations to foster dialogue with the Department. It also advises the Secretary on prospective policies and regulations and in many cases on their economic impact. The Private Sector Office promotes public-private partnerships and best practices to improve the nation's homeland security, and promotes Department policies to the private sector.	http://www.dhs.gov/about/structure/gc_1166220191042.shtm
Federal Business Opportunities (Fed Biz Opps)	"Virtual marketplace" that captures the official Federal government procurement opportunities allowing contractors to retrieve services posted by government buyers.	https://www.fbo.gov/
Small Business Innovation Research (SBIR)	SBIR is a set-aside program (2.5% of an agency's extramural budget) for domestic small business concerns to engage in Research/Research and Development (R/R&D) that has the potential for commercialization.	https://www.sbir.dhs.gov/
Small Business Assistance	Provides numerous resources, links and contacts to ensure that small companies have a fair opportunity to compete and be selected for Department of Homeland Security contracts.	http://www.dhs.gov/xopnbiz/smallbusiness/
Mentor-Protégé Program	Designed to motivate and encourage large business prime contractor firms to provide mutually beneficial developmental assistance to small business, veteran-owned small business, service-disabled veteran-owned small business, HUBZone small business, small disadvantaged business, and women-owned small business concerns.	http://www.dhs.gov/xopnbiz/smallbusiness/editorial_0716.shtm
SECURE (System Efficacy through Commercialization , Utilization, Relevance and Evaluation) Program	An efficient and cost-effective program to foster cooperative "win-win" partnerships between the U.S. Department of Homeland Security and the private sector. The Department works with the private sector to develop products, systems or services aligned to the needs of its operating components, first responders and critical infrastructure/key resources owners and operators – representing in many cases, large potential available markets.	http://www.dhs.gov/xres/program_s/gc_1211996620526.shtm

S&T Directorate – Homeland Security:

DHS and/or Federal Contact	Description	Contact Information
TechSolutions Program	Established to provide information, resources and technology solutions that address mission capability gaps identified by the emergency response community. The goal of TechSolutions is to field technologies that meet 80% of the operational requirement, in a 12 to 15 month time frame, at a cost commensurate with the proposal but less than \$1 million per project.	http://www.dhs.gov/xfrstresp/training/gc_1174057429200.shtm
SBIR	Please refer to the description above.	https://www.sbir.dhs.gov/
SAFETY (Support Anti-terrorism by Fostering Effective Technologies) Act	Part of the Homeland Security Act of 2002, the SAFETY Act encourages the development and deployment of anti-terrorism technologies to protect the nation and provide “risk management” and “litigation management” protections for sellers of qualified anti-terrorism technologies and others in the supply and distribution chain.	https://www.safe.tyact.gov/
Homeland Security Advanced Research Projects Agency (HSARPA)	Manages a broad portfolio of solicitations and proposals for the development of homeland security technology. HSARPA performs this function in part by awarding procurement contracts, grants, cooperative agreements, or other transactions for research or prototypes to public or private entities, businesses, federally funded research and development centers, and universities.	https://baa.st.dhs.gov/
SECURE Program	Please refer to the description above.	http://www.dhs.gov/xres/programs/gc_1211996620526.shtm
Unsolicited Proposals	Composed of several component agencies which handle different types of acquisitions. This Department has several resources, links and contacts if a given small company has products or services which may be of interest to one or more of DHS component agencies.	http://www.dhs.gov/xopnbiz/opportunities/editorial_0617.shtm

To put it simply, the Commercialization Office welcomes the prospect of working with all kinds of small businesses. In fact, we make it a point in ALL of our briefs/presentations to discuss small business opportunities as well as provide seminars and resources on how to raise capital and form strategic partnerships.

Appendix I: Commercialization Briefing to Industry

The following pages include slides used in briefing the private sector on business opportunities with DHS and its stakeholders.

Slide 1

Opportunities for the Private Sector



November 2009

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
Department of Homeland Security
Email: Thomas.Cellucci@dhs.gov
Website: <http://bit.ly/commercializationresources>

Slide 2

Discussion Guide

- Overview of Department of Homeland Security
- Commercialization Office Initiatives at DHS
- Capstone Integrated Product Teams (IPTs)
- Market Potential is Catalyst for Rapid New Product Development
- Getting on the Same Page
- SECURE Program
- Safety Act Protection
- TechSolutions
- SBIR Opportunities
- Getting Involved
- Effecting Change in Government
- Summary



Homeland Security

Slide 3

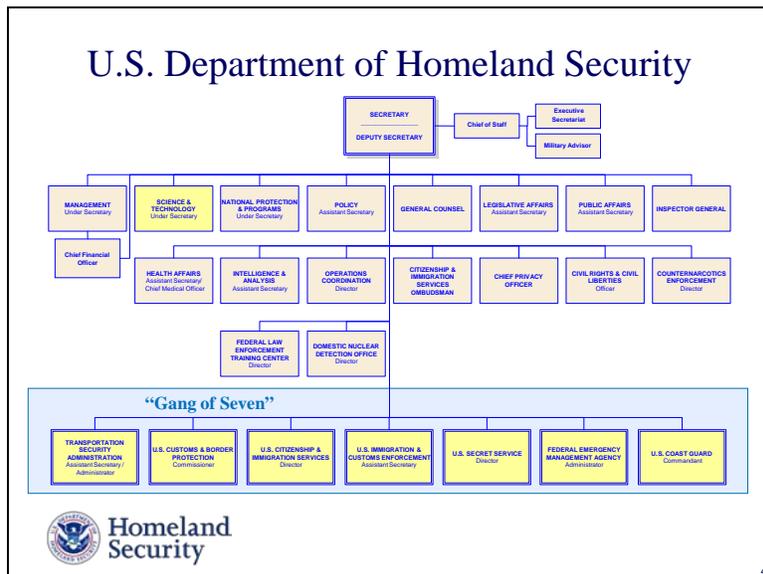
Homeland Security Mission



- Lead Unified National Effort to Secure America
- Prevent Terrorist Attacks Within the U.S.
- Respond to Threats and Hazards to the Nation
- Ensure Safe and Secure Borders
- Welcome Lawful Immigrants and Visitors
- Promote Free Flow of Commerce

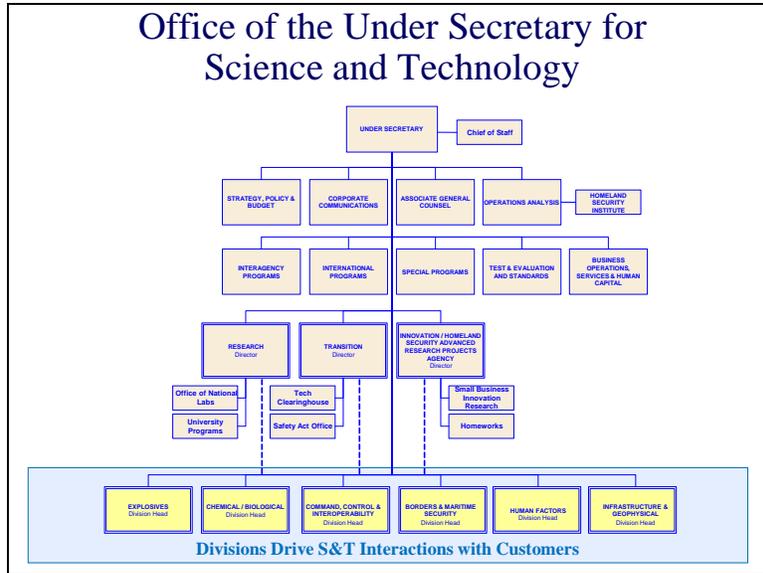


Slide 4



Department of Homeland Security Organization Chart

Slide 5



Office of the Under Secretary for Science and Technology organization chart

Slide 6

DHS S&T Goals

Consistent with the Homeland Security Act of 2002

- **Accelerate the delivery of enhanced technological capabilities** to meet the requirements and fill capability gaps to support DHS agencies in accomplishing their mission.
- Establish a lean and agile world-class S&T management team to deliver the technological advantage necessary to ensure DHS Agency mission success and prevent technological surprise.
- Provide leadership, research and educational opportunities and resources to develop the necessary intellectual basis to enable a national S&T workforce to secure the homeland.

Homeland Security

Slide 7

DHS S&T Investment Portfolio

Balance of Risk, Cost, Impact, and Time to Delivery

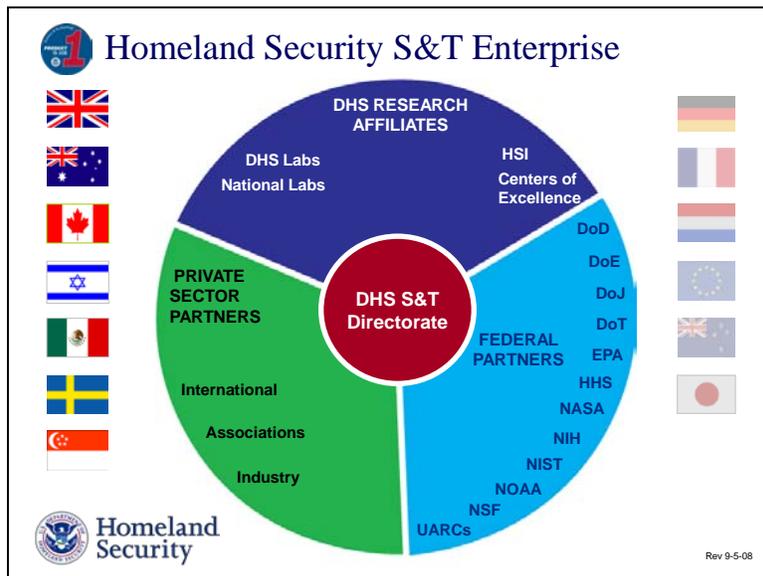
<p>Product Transition (0-3 yrs)</p> <ul style="list-style-type: none"> ▪ Focused on delivering near-term products/enhancements to acquisition ▪ Customer IPT controlled ▪ Cost, schedule, capability metrics 	<p>Innovative Capabilities (1-5 yrs)</p> <ul style="list-style-type: none"> ▪ High-risk/High payoff ▪ “Game changer/Leap ahead” ▪ Prototype, Test and Deploy ▪ HSARPA
<p>Basic Research (>8 yrs)</p> <ul style="list-style-type: none"> ▪ Enables future paradigm changes ▪ University fundamental research ▪ Gov’t lab discovery and invention 	<p>Other (0-8+ yrs)</p> <ul style="list-style-type: none"> ▪ Test & Evaluation and Standards ▪ Laboratory Operations & Construction ▪ Required by Administration (HSPDs) ▪ Congressional direction/law

Customer Focused, Output Oriented

Homeland Security

7

Slide 8

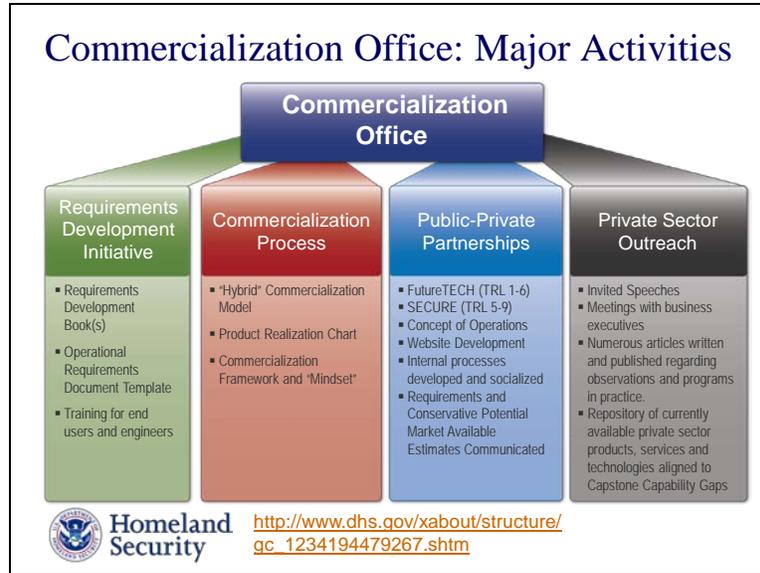


S&T has seven formal bilateral agreements with key partner nations, shown at left, with five others – including Germany -- in the works.

Homeland security is not a Federal effort, but a national effort that cuts across disciplines and jurisdictions and includes partners from academia, industry and all levels of government.

This chart depicts the many research partners of DHS S&T that encompass the broader research, private sector and government communities.

Slide 9



Slide 10

Commercialization Office Highlights:

- White House Office of Science and Technology Policy briefings (Chief Technology Officer Aneesh Chopra)
- Homeland Security Council: Recommended priority for FY11-15 for transportation security: SECURE Program
- Inclusion of Commercialization processes into DHS Acquisition Management Directive MD 102-01 (scheduled release September 2009)
- Homeland Security Advisory Council, Essential Technology Task Force Report June 2008
- Council on Competitiveness, Chief Commercialization Officer is first Federal Government Representative
- "Big Bang Economics": CNN Feature Video with Jeanne Meserve
- "Burned, Baked and Blown Up": Reuters Video with Rob Muir
- Two Federal Certification Programs developed and implemented—SECURE™ and FutureTECH™: Innovative public-private partnerships
- Published Five books (and more than 20 articles) on requirements development and public-private partnerships

 **Homeland Security**

10

Slide 11

Three Step Approach: Keep it Simple and Make it Easy

- 1 Develop Detailed Requirements
And Relay Conservative Market Potential
- 2 Establish Strategic Partnerships
 - Business Case Information
 - Open Competition
 - Detailed Mutual Responsibilities
- 3 Deliver Products!



11

Slide 12

Two Models for Product Realization

Big-A Acquisition

1. Requirements derived by Government
2. RFP and then cost-plus contract(s) with developer(s) (which incentivizes long intervals)
3. Focus on technical performance
4. Production price is secondary (often ignored)
5. Product price is cost-plus
6. Product reaches users via Government deployment

Performance is King

Relationship between end users and product developer is usually remote

?

Pure Commercialization

1. Requirements derived by Private Sector
2. Product development funded by the developer (which incentivizes short intervals)
3. Technical performance secondary (often reduced in favor of price)
4. Focus on price point
5. Product price is market-based
6. Product reaches users via marketing and sales channels

Performance/Price is King

Relationship between end users and product developer is crucial

Is there a "Middle Ground"?



12

Slide 13

A new model for Commercialization...

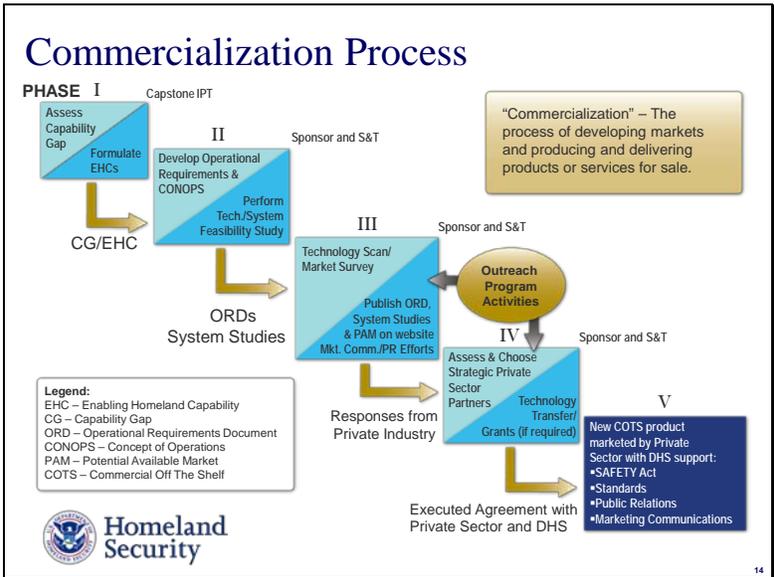
1. Development of Operational Requirements Document (ORD)
2. Assess addressable market(s)
3. Publish ORD and market assessment on public DHS web portal, soliciting interest from potential partners
4. Execute no-cost agreement (streamlined CRADA) with multiple Private Sector entities, transferring technology (if necessary)
5. Develop supporting grants and standards as necessary
6. Assess T&E after product is developed
7. New Commercial off the Shelf (COTS) product marketed by Private Sector with DHS support

Differences from the Acquisition model:

- Primary criteria for partner selection is market penetration, agility, and performance/price ratio
- Product development is not funded by DHS
- Government involvement is limited to inherently governmental functions (e.g., Grants and Standards)

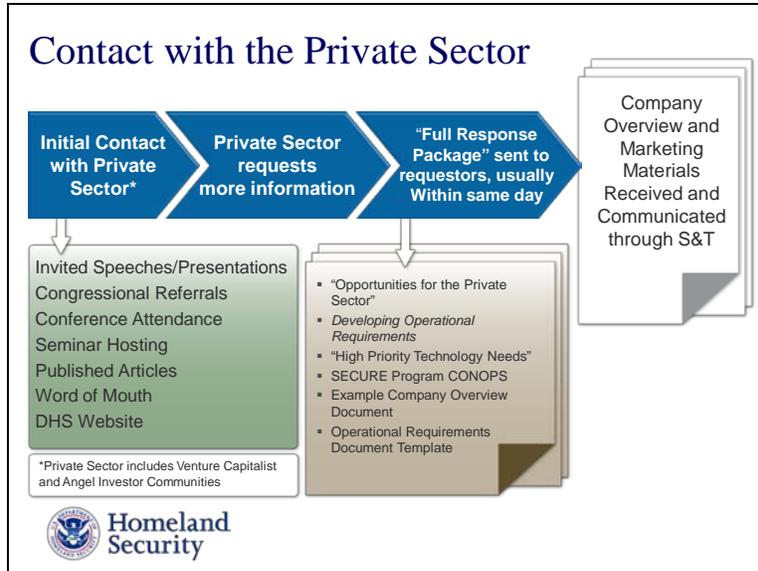


Slide 14

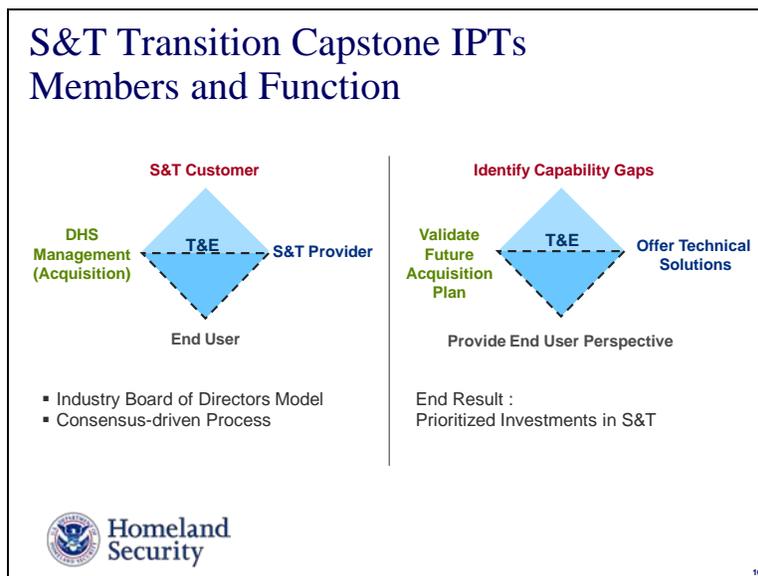


The new Commercialization Process is a hybrid model that combines processes from both the “pure Acquisition” model and the “pure Commercialization” model.

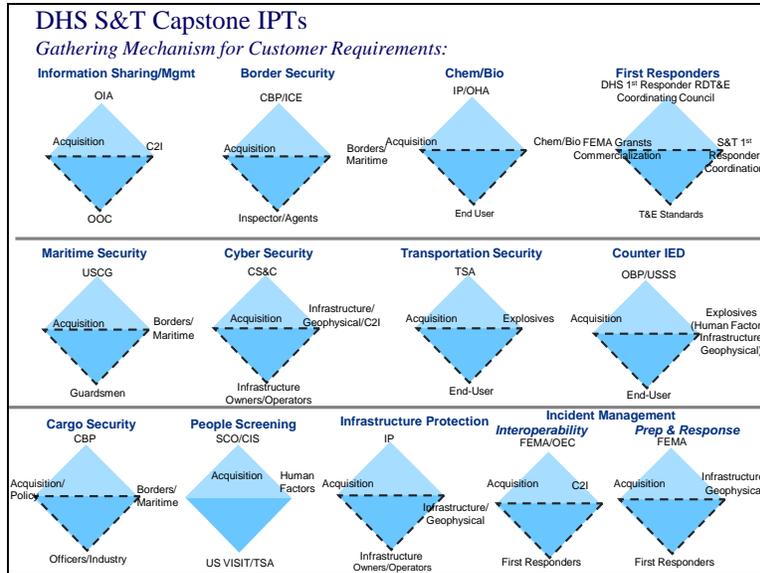
Slide 15



Slide 16



Slide 17



Slide 18

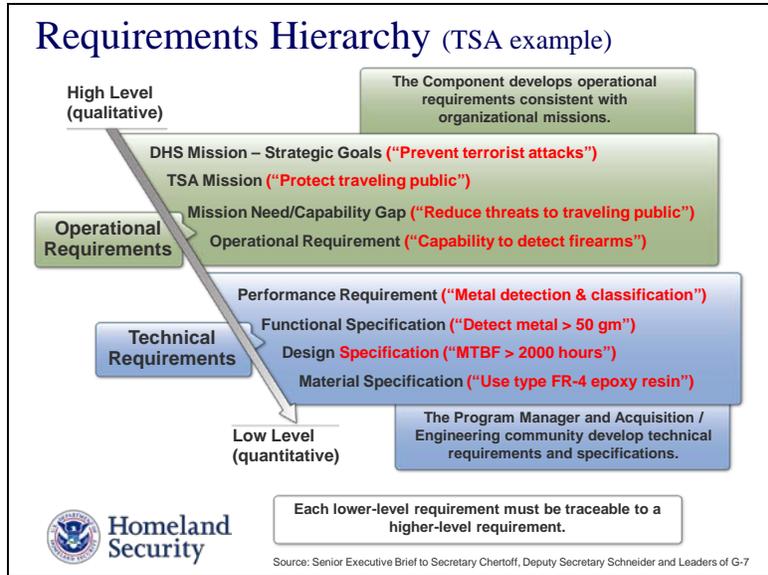
Cargo Security

Representative Technology Needs

- Enhanced screening and examination by non-intrusive inspection
- Increased information fusion, anomaly detection, Automatic Target Recognition capability
- Detect and identify WMD materials and contraband
- Capability to screen 100% of air cargo
- Test the feasibility of seal security; detection of intrusion
- Track domestic high-threat cargo
- Harden air cargo conveyances and containers
- Positive ID of cargo and detection of intrusion or unauthorized access

Source: S&T High Priority Technology Needs, May 2007

Slide 19



- The requirements hierarchy is naturally divided into two domains, operational and technical. The Sponsor, representing the operators, is responsible for all operational requirements. The technical system developer is responsible for all technical requirements.
- The Mission Needs Statement is the entry point to Acquisition.
- During an Acquisition program, requirements and specifications of increasing detail will ultimately specify the materiel solution. All lower-level requirements must be traceable to higher-level requirements. If not, why are they required?
- The development of these requirements and specifications is governed by the systems engineering process.
- Attention to detail, and disciplined adherence to process, is required for a successful Acquisition program. Counter-examples are legion.

Slide 20

ORD: Operational Requirements Document

What: ORDs provide a clear definition and articulation of a given problem.

How: Training materials have been developed to assist drafting an ORD.

- *Developing Operational Requirements*, 353pp. Available online: http://www.dhs.gov/xlibrary/assets/Developing_Operational_Requirements_Guides.pdf

When: For Use in Acquisition, Procurement, Commercialization and Outreach Programs –Any situation that dictates detailed requirements (e.g. RFQ, BAA, RFP, RFI, etc.)

Why: It's cost-effective and efficient for both DHS and all of its stakeholders.







20

Slide 21

Generating “Good” ORDs

- Solution Agnostic
- Take into account the varying needs and wants of markets/market segments

Define Problem
↓
Conduct Research
↓
Data Collection
↓
Interpret and Analyze

Verify results to reach consensus-based articulation of the problem
“Strive for excellence, not perfection!”

Homeland Security

Source: Kaufman, et. al.

21

Slide 22

Interlinking Mechanisms Create Conversations Pipelines

The “Neural Net”

Requirements
↓
Acquisition
↓
Technology Development
↓
Resources (People, Systems, Hardware, Capital, Technology)
↓
Requirements

Government Stakeholders
— Congress,
— GAO,
— OMB,
— Int’l Org.,
— Other Gov’t Agencies

Industry

Output Capabilities

John Higbee
Director,
Acquisition Program
Management Division

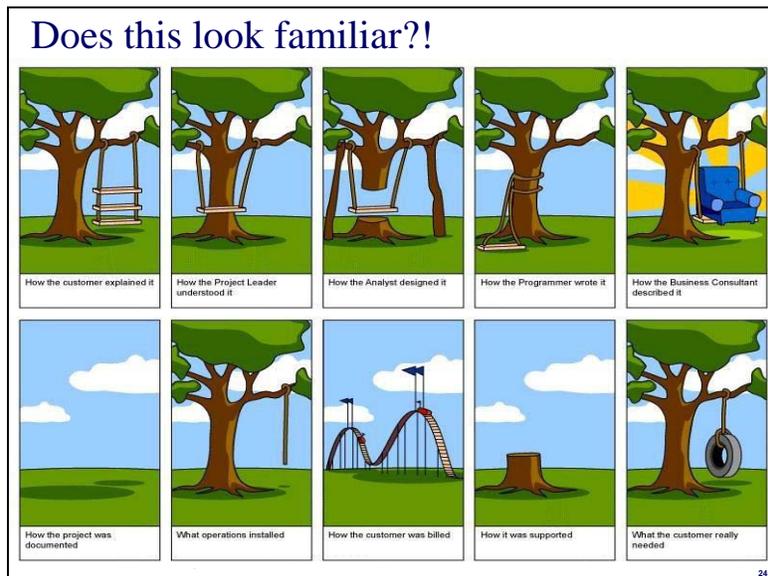
Homeland Security

22

Slide 23



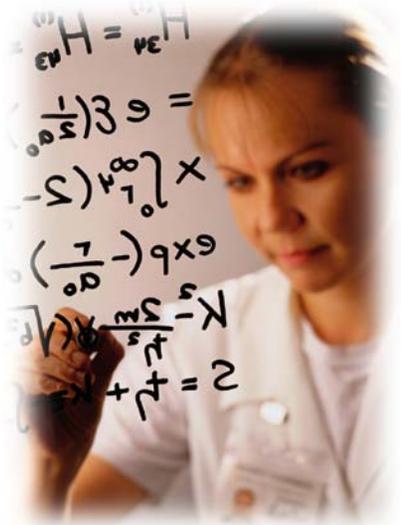
Slide 24



Slide 25

Getting on the “Same Page”

- Historical Perspective
- Language is Key
- Communication is Paramount



$$E\mathbf{H} = \nabla \times \mathbf{H}$$

$$\left(\frac{1}{\epsilon_0}\right) \rho = \nabla \cdot \mathbf{E}$$

$$\left(\frac{1}{\mu_0}\right) \mathbf{j} = \nabla \times \mathbf{A}$$

$$\nabla^2 \mathbf{A} = -\mu_0 \mathbf{j}$$

$$\nabla \cdot \mathbf{A} = 0$$



Slide 26

Technology Readiness Levels (TRLs): Overview

TRLs are NASA-generated and Used Extensively by DoD

Basic principles observed and reported	1	Basic
Technology concept and/or application formulated	2	
Analytical and experimental critical function and/or characteristic	3	
Component and/or breadboard validation in laboratory environment	4	Advanced
Component and/or breadboard validation in relevant environment	5	
System/subsystem model or prototype demonstration in a relevant environment	6	Applied
System prototype demonstration in an operational environment	7	
Actual system completed and 'flight qualified' through test and demonstration	8	
Actual system 'flight proven' through successful mission operations	9	

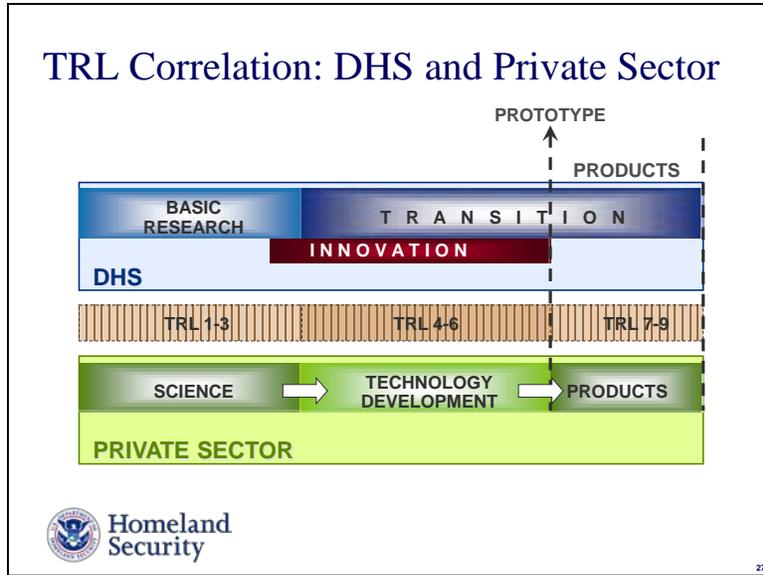
TECHNOLOGY MATURITY





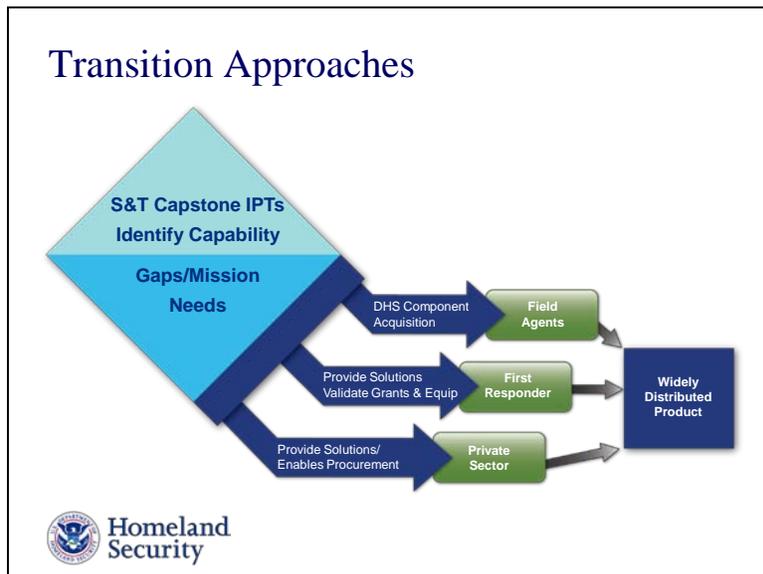
26

Slide 27

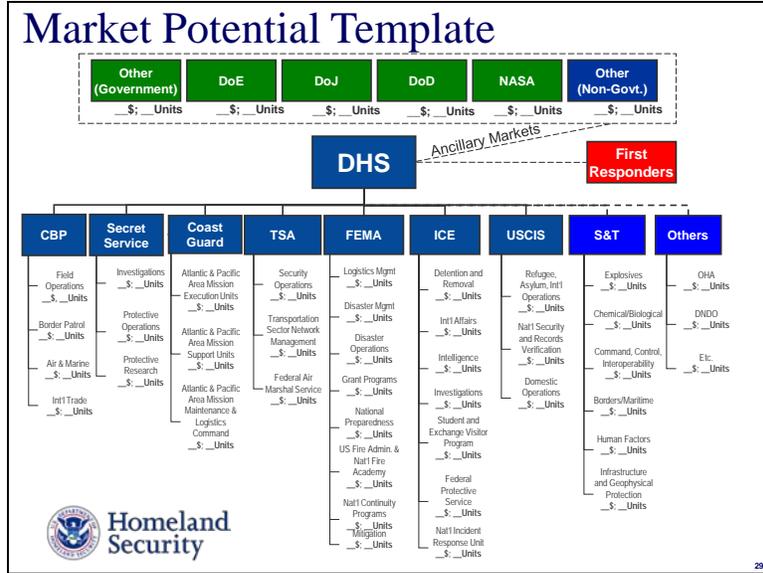


This view graph depicts the various lexicons used to describe product development life-cycles.

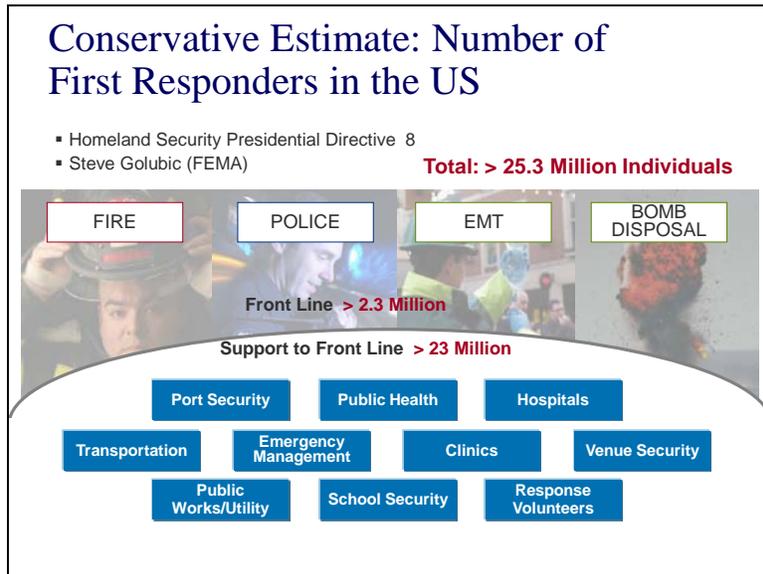
Slide 28



Slide 29



Slide 30



Slide 33

Call to Action: Mutual Benefits Create “Win-Win-Win” Relationships

Learn Current DHS Needs

Visit www.FedBizOpps.gov and <https://baa.st.dhs.gov> for current solicitations

Interact with DHS

Establish Mutually-beneficial Relationship

Inform DHS of Products/Capabilities

Request DHS – S&T Full Response Package at thomas.cellucci@dhs.gov

33

Slide 34

SECURE™ Program

Developing Solutions in Partnership with the Private Sector

- “Win-Win-Win” Public-Private Partnership program benefits DHS’s stakeholders, private sector and –most importantly- the American Taxpayer
- Saves time and money on product development costs leveraging the free-market system and encouraging the development of widely distributed products for DHS’s stakeholders
- Detailed articulation of requirements (using MD 102-01 ORD template) and T&E review provides assurance to DHS, First Responders and private sector users (like CIKR) that products/services perform as prescribed

http://www.dhs.gov/xres/programs/gc_1211996620526.shtm

34

Slide 35

SECURE™ Program

Concept of Operations



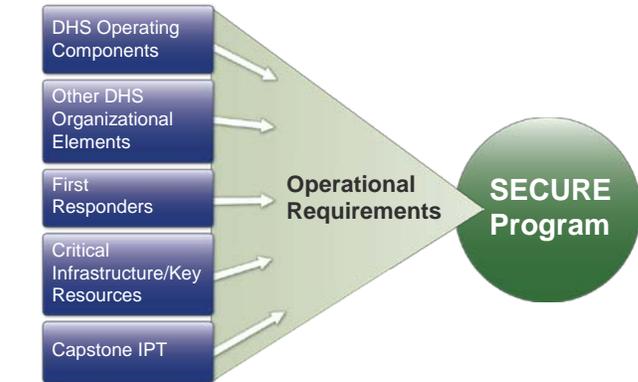
- **Application** – Seeking products/technologies aligned with posted DHS requirements
- **Selection** – Products/Technologies TRL-5 or above, scored on internal DHS metrics
- **Agreement** – One-page streamlined CRADA document. Outlines milestones and exit criteria
- **Publication of Results** – Independent Third-Party T&E conducted on TRL-9 product/service. Results verified by DHS, posted on DHS web-portal

Benefits:

- Successful products/technologies share in the imprimatur of DHS
- DHS Operating Components and First Responders make informed decisions on products/technologies aligned to their stated requirements
- DHS spends less on acquisition programs → Taxpayers win.

Slide 36

Input Function for SECURE™



Operational Requirements

SECURE Program



36

Slide 37

Why SECURE™ Program?

- **Multi-Use**
 - Provides private sector, in an open and transparent way, with what they need most—Business Opportunities
 - Provides assurance to DHS, First Responders and private sector users (like CI/KR) that products/services perform as prescribed (and provides vehicle for First Responders, CI/KR owners and operators to voice their requirements)
 - Augments the value of the SAFETY Act
- **Saves Money**
 - Private Sector uses its own resources to develop products and services to the benefit of the taxpayer and the Federal Government
- **Creates Jobs**
 - Detailed articulation of requirements coupled with funded large, potential available markets yield OPPORTUNITY that yields Job Creation (it's better to teach a person to fish than to give them a fish)
 - Enables small firms with innovative technologies to partner with larger firms, VCs and angel investors because of the credibility of having government show detailed requirements with associated market potential (instead of just their own business plans).
- **Efficient Use of Government Funds**
 - Articulating detailed requirements saves time and money. It is better for Government to spend funds to procure products or services that are available for sale and rigorously tested compared to spending money and time to develop new solutions for ill-defined problems.



Homeland Security

37

Slide 38

SECURE™ Program

Benefit Analysis “Win-Win-Win”

Taxpayers	Private Sector	Public Sector
1. Citizens are better protected by DHS personnel using mission critical products	1. Save significant time and money on market and business development activities	1. Improved understanding and communication of needs
2. Tax savings realized through Private Sector investment in DHS	2. Firms can genuinely contribute to the security of the Nation	2. Cost-effective and rapid product development process saves resources
3. Positive economic growth for American economy	3. Successful products share in the “imprimatur of DHS”; providing assurance that products really work	3. Monies can be allocated to perform greater number of essential tasks
4. Possible product “spin-offs” can aid other commercial markets	4. Significant business opportunities with sizeable DHS and DHS ancillary markets	4. End users receive products aligned to specific needs
5. Customers ultimately benefit from COTS produced within the Free Market System – more cost effective and efficient product development	5. Commercialization opportunities for small, medium and large business	5. End users can make informed purchasing decisions with tight budgets



Homeland Security

38

Slide 39

FutureTECH™ Program

Addressing the Future Needs of DHS

- ‘Win-Win-Win’ Public-Private Partnership program benefits DHS stakeholders, private sector and –most importantly- the American Taxpayer
- 5W template provides detailed overview of Critical Research/Innovation Focus Areas
- Critical Research/Innovation Focus Areas provide universities, national labs and private sector R&D organizations insight into the future needs of DHS stakeholders
- Partnership program encourages R&D organizations to work on development of technology solutions up to TRL-6 to address long-term DHS needs.



http://www.dhs.gov/xres/programs/gc_1242058794349.shtm



39

Slide 40

FutureTECH™ Program

Concept of Operations



- Expression of Interest – Seeking technologies aligned with posted DHS Critical Research and Innovation Focus Areas
- Acceptance–Technologies TRL-6 or below, scored on internal DHS metrics
- CRADA– One-page CRADA document. Outlines milestones and exit criteria
- Publication of Results – Independent Third-Party T&E conducted on TRL-6 technology. Results verified by DHS, posted on DHS web-portal

Benefits:

- Insight into future needs of DHS Stakeholders
- Increased speed-of-execution of technology development and transition
- DHS spends less on technology development → Taxpayers win.



40

Slide 41

FutureTECH™ Program

Critical Research & Innovation Focus Areas

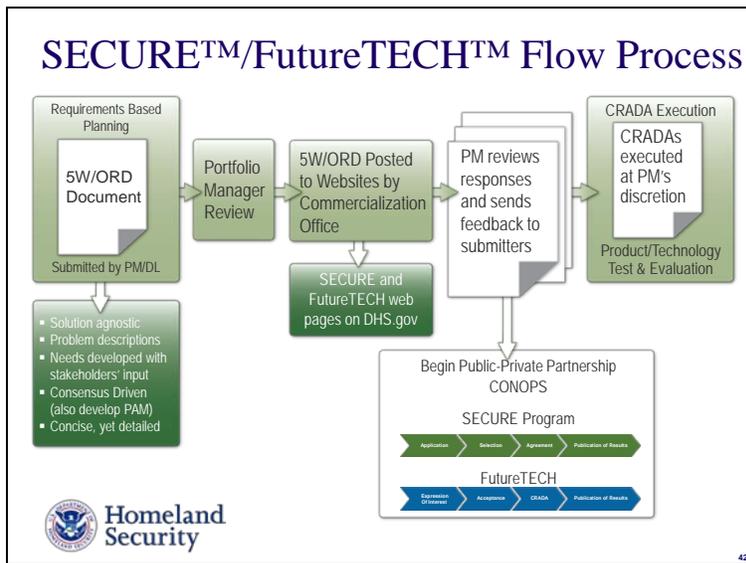
- Improvised Explosive Devices Detect & Defeat Countermeasures:
 - Waterborne IEDs
 - Vehicle Borne IEDs
 - Radio Controlled IEDs
 - Person Borne IEDs
 - IED Assessment and Diagnostics
 - IED Access and Defeat
 - Homemade Explosives
- IED Threat Characterization
- IED Mitigation: Alert/Warning System
- IED Deter and Predict: Network Attack and Analysis



Homeland Security

41

Slide 42



FutureTECH is initiated by PM or DL through submission of 5Ws Document outlining a Critical Research/Innovation Focus Area. Portfolio Manager reviews for accuracy/approval. Commercialization Office places 5Ws on website (with PM's contact information). Reviews conducted by PM (or designee) within 4-6 weeks with feedback sent directly to submitter (with copy to Ryan Policy at ryan.policay@associates.dhs.gov). Any CRADAs are at the total discretion of the PM.

Slide 43



How to navigate to the SECURE Program website. Direct website link:
http://www.dhs.gov/xres/programs/gc_1211996620526.shtm

Slide 44

Federal Business Opportunities

Sites where the Office of Procurement Operations (OPO) posts opportunities for prospective suppliers to offer solutions to DHS – S&T's needs:

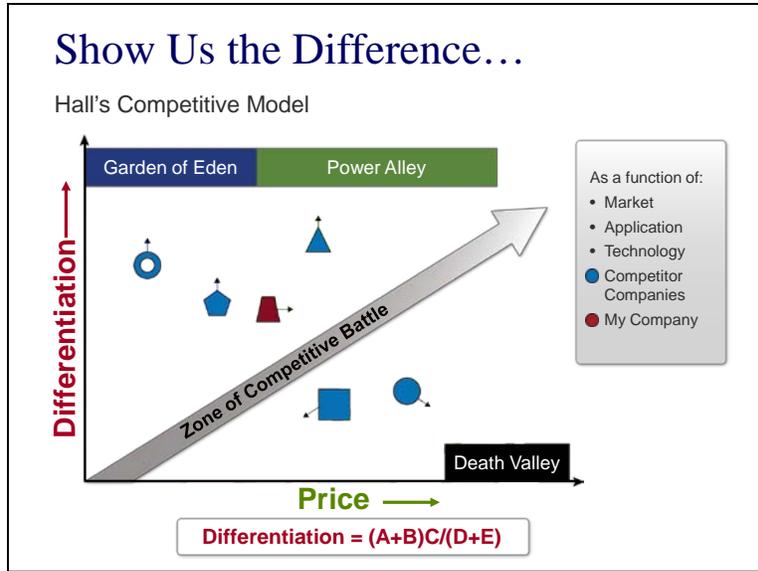
- www.FedBizOpps.gov
- <https://baa.st.dhs.gov/>
- <https://www.sbir.dhs.gov/>
- www.Grants.gov

take advantage of...

- **Vendor Notification Service:** Sign up to receive procurement announcements and solicitations/BAA amendment releases, and general procurement announcements.
<http://www.fedbizoppes.gov>
- **S&T's Solicitation Portal:** The Department of Homeland Security Science and Technology Directorate currently has several active Solicitations on a broad range of topics. Relevant information is posted and access to the teaming portal, conference registration and white paper/proposal registration and submission is provided, as applicable. In addition, historical information about past Solicitations and Workshops is maintained.
<https://baa.st.dhs.gov>
- **Truly Innovative and Unique Solution:** Refer to Part 15.6 of the Federal Acquisition Regulation (FAR) which provides specific criteria that must be met before a unsolicited proposal can be submitted to Diane Osterhus.
<http://www.acquisition.gov/far/current/html/Subpart%2015.6.html>
- **EAGLE Contract** will serve as a department-wide platform for acquiring IT service solutions.
http://www.dhs.gov/xopnbiz/opportunities/editorial_0700.shtm

Contact Information:
 Diane Osterhus
 Department of Homeland Security
 Office of the Chief Procurement Officer
 245 Murray Dr., Bldg. 410
 Washington, DC 20528
unsolicited.proposal@dhs.gov
 202-447-5576

Slide 45



The Hall's Competitive Model shows in a graphical way the way in which companies can create differentiation. The "variables" contained in the differentiation "formula" are different user defined factors that need to be considered when comparing a product/technology/market against other similar items.

Slide 46

More Opportunities with DHS
Science and Technology

Slide 47

SAFETY Act

Support Anti-Terrorism by Fostering Effective Technologies Act of 2002

- Enables the development and deployment of qualified anti-terrorism technologies
- Provides important legal liability protections for manufacturers and sellers of effective technologies
- Removes barriers to industry investments in new and unique technologies
- Creates market incentives for industry to invest in measures to enhance our homeland security
- The SAFETY Act liability protections apply to a vast range of technologies, including:
 - Products
 - Services
 - Software and other forms of intellectual property (IP)

Examples of eligible technologies:

- Threat and vulnerability assessment services
- Detection Systems
- Blast Mitigation Materials
- Screening Services
- Sensors and Sensor Integration
- Vaccines
- Metal Detectors
- Decision Support Software
- Security Services
- Data Mining Software

Protecting You, Protecting U.S.

Additional SAFETY Act information...
Online: www.safetyact.gov Email: helpdesk@safetyact.gov Toll-Free: 1-866-788-9318

Slide 48

Long Range Broad Agency Announcement

(Contact: Adrian.Groth@hq.dhs.gov | <https://baa.st.dhs.gov/>)

- Peer or scientific review of proposals in Basic Research and Applied Technology in science and engineering.
- Research to promote revolutionary changes in technologies; advance the development, testing, and deployment of security technologies; and to accelerate the prototyping and deployment of technologies.
- Streamlined and flexible funding mechanism. Open to all DHS-relevant ideas, no submission deadlines, no ceiling on potential funding.
- Public Solicitation identifies science and technology target areas as does the S&T publication "High Priority Technology Needs" dated May 2009, as amended. This document may be obtained by accessing <https://baa.st.dhs.gov> and by following the link for "Representative High Priority Technology Needs".

* Peer or Scientific Reviews *
* Basic or Applied Research *
* Maximum Flexibility: Schedules, Subjects, Funding *

 **Homeland Security**

48

Slide 49

Technology Transfer

Transfer federally owned/originated technology to State and local governments and the private sector, ensuring the widest dissemination and impact of Federal research investments.

DOD 1401 Program Liaison

- Push DHS requirements to DOD
- Pull DOD technologies into DHS for first responders
- Assess technology suitability and adaptations for DHS applications
- Create DHS & DoD Program Manager partnerships to maximize technology enhancements for our nation's first responders

Office of Research and Technology Applications (ORTA)

- Manage all technology transfer mechanisms used in DHS
 - Cooperative Research and Development Agreements (CRADAs)
 - Licensing Agreements
 - Other Transaction Agreements (OTAs)
 - Commercial Test Agreements
 - Work for Others
 - Partnership Intermediaries
- Capture Intellectual Property and licensing in DHS
- Assess R&D projects for potential commercial applications
- Train engineers and scientists for Technology Transfer and Intellectual Property
- Represent DHS in the Federal Laboratory Consortium

Contact: Marlene Owens, Marlene.Owens@dhs.gov

Slide 50

The screenshot shows the DHS SBIR Program website. The URL in the browser is <https://www.sbir.dhs.gov>. The page title is "Department of Homeland Security - Science & Technology Directorate - SBIR Program - Microsoft Internet Explorer". The main content area is titled "Department of Homeland Security Science and Technology Directorate (S & T Directorate) Small Business Innovation Research (SBIR) Program".

Three red callout boxes are overlaid on the page:

- Safety Act**: Points to the "Safety Act" link in the top navigation bar.
- Other Funding Opportunities**: Points to the "Other Funding Opportunities" link in the top navigation bar.
- Topic Recommendations**: Points to the "Topic Recommendations" link in the top navigation bar.

The main content area contains text about the DHS S&T SBIR Program, including information about solicitation topics, the Cost Match feature, and the Phase I award process.

Slide 51

TechSolutions

The mission of TechSolutions is to rapidly address technology gaps identified by Federal, State, Local, and Tribal first responders

- Field prototypical solutions in 12 months
- Cost should be commensurate with proposal but less than \$1M per project
- Solution should meet 80% of identified requirements
- Provide a mechanism for Emergency Responders to relay their capability gaps
 - Capability gaps are gathered using a web site (www.dhs.gov/techsolutions)
- Gaps are addressed using existing technology, spiral development, and rapid prototyping
- Emergency Responders partner with DHS from start to finish

Rapid Technology Development
Target: Solutions Fielded within 1 year, at <\$1M



51

Slide 52

Getting Involved: S&T Contacts

Division	Email
Jim Tuttle	SandT.Explosives@dhs.gov
Beth George	SandT.ChemBio@dhs.gov
David Boyd	SandT.CCI@dhs.gov
Anh Duong	SandT.BordersMaritime@dhs.gov
Sharla Rausch	SandT.HFD@dhs.gov
Chris Doyle	SandT.IGD@dhs.gov
Rich Kikla	SandT.Transition@dhs.gov
Starnes Walker	SandT.Research@dhs.gov
Roger McGinnis	SandT.Innovation@dhs.gov



52

Slide 53

Summary

Detailed Requirements
Sizeable Market Potential
Delivered Products – PERIOD!

How Can You Afford NOT to Partner with DHS?

Questions/Comments:
Thomas A. Cellucci, Ph.D., MBA
thomas.cellucci@dhs.gov



53

Slide 54

U.S. Department of Homeland Security: Science and Technology Directorate's Chief Commercialization Officer

Dr. Cellucci accepted a five-year appointment from the Department of Homeland Security in August 2007 as the Federal Government's first Chief Commercialization Officer (CCO). He is responsible for initiatives that identify, evaluate and commercialize technology for the specific goal of rapidly developing and deploying products and services that meet the specific operational requirements of the Department of Homeland Security's Operating Components and other DHS stakeholders such as First Responders and Critical Infrastructure/Key Resources owners and operators. Cellucci has also developed and continues to drive the implementation of DHS S&T's outreach with the private sector to establish and foster mutually beneficial working relationships to facilitate cost-effective and efficient product/service development efforts. His efforts led to the establishment of the DHS S&T Commercialization Office in October 2008. The Commercialization Office is responsible for four major activities: a requirements development initiative for all DHS stakeholders, the development and implementation of a commercialization process for DHS, development and execution of private sector partnership programs such as SECURE and leading the private sector outreach for the S&T Directorate.



Since his appointment, he has published three comprehensive guides [*Requirements Development Guide* (April 2008), *Developing Operational Requirements* (May 2008), and *Developing Operational Requirements, Version 2* (November 2008)] dealing with the development of operational requirements, developed and implemented a commercialization model for the entire department and established the SECURE Program—an innovative public-private partnership to cost-effectively and efficiently develop products and services for DHS's Operating Components and other DHS stakeholders. In addition, he has written over 25 articles and a compilation of works [*Harnessing the Valuable Experiences and Resources of the Private Sector for the Public Good* (February 2009)] geared toward the private sector to inform the public of new opportunities and ways to work with DHS. Cellucci has received recognition for his outreach efforts and engagement with the small and disadvantaged business communities who learn about potential business opportunities and avenues to provide DHS with critical technologies and products to help secure America. Cellucci is an accomplished entrepreneur, seasoned senior executive and Board member possessing extensive corporate and VC experience across a number of worldwide industries. Profitably growing high technology firms at the start-up, mid-range and large corporate level has been his trademark. He has authored or co-authored over 139 articles on Requirements development, Commercialization, Nanotechnology, Laser physics, Photonics, Environmental disturbance control, MEMS test and measurement, and Mistake-proofing enterprise software. He has also held the rank of Lecturer or Professor at institutions like Princeton University, University of Pennsylvania and Camden Community College. Cellucci also co-authored ANSI Standard Z136.5 "The Safe Use of Lasers in Educational Institutions". Dr. Cellucci is also a commissioned Admiral and Commander of a Squadron in Texas responsible for civil defense and has been a first responder for over twenty years. As a result of his consistent achievement in the commercialization of technologies, Cellucci has received numerous awards and citations from industry, government and business. In addition, he has significant experience interacting with high ranking members of the United States government—including the White House, US Senate and US House of Representatives—having provided executive briefs to three Presidents of the United States and ranking members of Congress. Cellucci represents DHS as the first Federal Government member on the U.S. Council on Competitiveness.

Cellucci earned a PhD in Physical Chemistry from the University of Pennsylvania, an MBA from Rutgers University and a BS in Chemistry from Fordham University. He has also attended and lectured at executive programs at the Harvard Business School, MIT Sloan School, Kellogg School and others. Dr. Cellucci is regarded as an authority in rapid time-to-market new product development and is regularly asked to serve as keynote speaker at both business and technical events.

Slide 55



Appendix J: Acquisition Training Mini-Course

Acquisition and Commercialization

How DHS develops end-user capabilities



Sam Francis (instructor)

samuel.francis@associates.dhs.gov

[date of class]



revised 4/14/09

- This mini-course is one of a series, sponsored by the Deputy Under Secretary, S&T.
- The material takes an hour to cover, and will start and stop on time, so make sure any questions are for general clarification. The speaker will remain for 30 minutes after the end for discussion, if desired for questions which are more specific in nature.
- Hard copies of the slides will be handed out. The slides are also available from the RDT&E web site (click on Training and follow your nose). To browse the RDT&E web site, double-click on "Shared\RDT&E Process Website\index.htm" (then bookmark).
- Please sign the sign-in sheet.
- Today we'll be talking about Acquisition and Commercialization, which are the principal methods DHS uses to develop capabilities in the field.
- The term "acquisition" can be confusing because the word is used to mean different things and is often confused with procurement. The next slide addresses this confusion.

Big “A” and little “a” Acquisition

Think
“cradle
to grave”

Big “A” Acquisition (sometimes called “program acquisition”) is a requirements-based process that encompasses the complete system life cycle, including planning, needs analysis, analysis of alternatives, systems engineering, technology and system development, test and evaluation, logistics support, production, deployment, operation, and maintenance.

Think
“procurement”

Little “a” acquisition (also called “stand-alone acquisition”) is the procurement of goods and services. It plays a role in Big-A Acquisition, but should not be confused with it.

Our customers are responsible for Big-A, and we must understand it in order to support them.

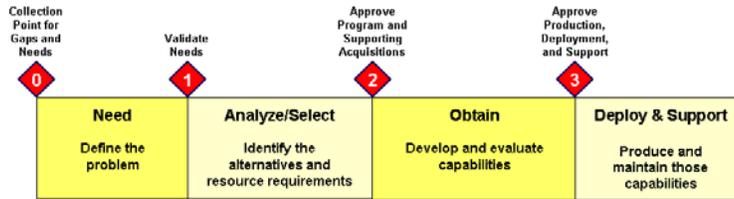


Homeland
Security

2

- “Acquisition” is one of those words, like “research”, “transition,” “program,” and “project” which are in the common vernacular and used by different people to mean different things. Where precision is useful, these words have to be defined more precisely. So let’s avoid some confusion by defining the two contexts in which the word “acquisition” is used.
- Little-“a” acquisition is basically a procurement action to buy existing products or services. OPO requires documentation (e.g., an acquisition plan and an alternatives analysis) to demonstrate that you’ve thought through what you’re buying and are making good choices, but it’s a relatively straightforward and low-risk procurement.
- Big-“A” acquisition is a process to acquire a product or system which must be developed to a set of requirements. It’s much higher-risk than Little-“a” acquisition, and requires disciplined program management to manage the risk and assure the outcome.
- In short, Little-“a” acquisition is buying stuff that exists, and Big-“A” acquisition is buying stuff that doesn’t yet exist.

DHS Acquisition Life Cycle



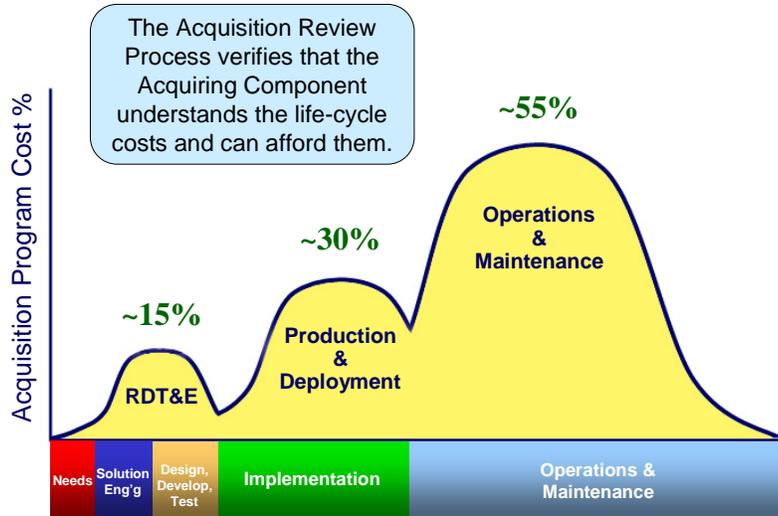
- Acquisition Decision Authority (ADA) is the gatekeeper at each Acquisition Decision Event (ADE)
 - Level 1 (LCC > \$1B): DepSec at ADE 1, USM at ADE 2, USM/DUSM at ADE 3
 - Level 2 (\$300M < LCC < \$1B): Same as Level 1 but can be delegated
 - Level 3 (\$50M < LCC < \$300M): Component Head at ADE 1, ADA-equivalent afterwards
- Certain documents are mandated at each ADE
 - ADE 1: Mission Needs Statement, Capability Development Plan
 - ADE 2: Concept of Operations, Operational Requirements Document, Acquisition Program Baseline, Acquisition Plan, Integrated Logistics Support Plan, Analysis of Alternatives, Life Cycle Cost Estimate, Test and Evaluation Master Plan



3

- DHS has codified a very simple Acquisition Life Cycle Framework in Acquisition Directive 102-01. It's a phase-gate process in which the number of phases is kept to a bare minimum, described by the plain English terms "Need," "Analyze/Select," "Obtain," and "Deploy & Support."
- The Acquisition Life Cycle Framework is punctuated by gates (called Acquisition Decision Events, or ADEs) at the beginning of each phase, at which gatekeepers assure that the Acquisition program has satisfied certain planning and execution requirements. The seniority of the gatekeeper depends on the size of the Acquisition program. The gates are the control points of the Acquisition framework. The series of gates, which enforce disciplined program management, is called the Acquisition Review Process (ARP).
- The Acquisition Life Cycle Framework doesn't tell a program manager how to run a program, but does insist on certain documents which reflect good planning. For example, at ADE 1, the program manager must have an authorized need (documented in a Mission Need Statement) and an approved plan (called a Capability Development Plan) for developing the needed capability.
- Templates are provided for all the Acquisition documentation required by Acquisition Directive 102-01.

Life-Cycle Costs are dominated by the “logistics tail”

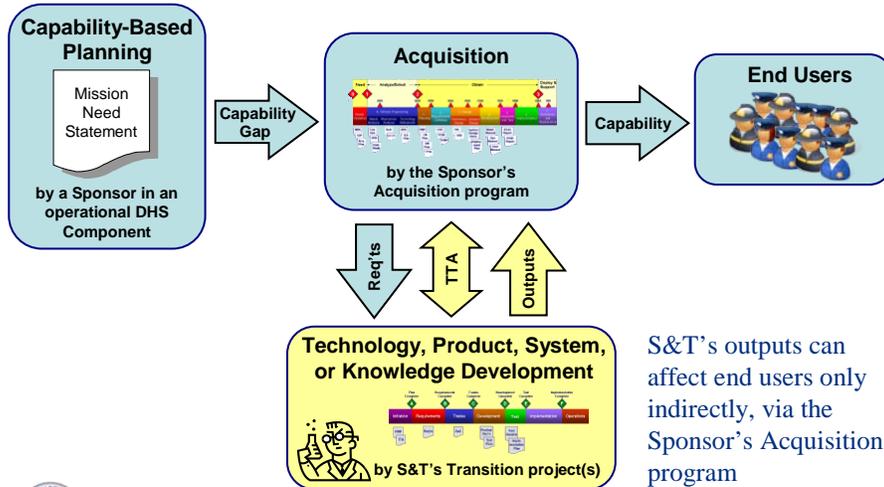


Homeland Security

4

- There's little point doing RDT&E to develop a system if the Sponsor can't afford the life-cycle costs. For most systems the majority of cost is incurred during Production, Deployment, Operations, and Maintenance (called “Deploy & Support” in the DHS Acquisition life cycle).
- The Sponsor of an Acquisition program to create a Business Case (typically, an Exhibit 300), forcing the Sponsor to consider the entire life cycle. If S&T is responsible for the RDT&E phases, the Sponsor needs S&T's help in estimating the life-cycle costs.
- The DHS system development life cycle doesn't explicitly include disposal costs, but they may be sizeable and should not be ignored.

Big-A Acquisition is the path to the end users supported by S&T



- The blue boxes show the primary path from mission needs to an enhanced capability in the field. The Acquisition Life Cycle Framework is DHS's high-level methodology for developing such a capability. The Acquisition sponsor is the champion for the end users, and specifies the problem (the mission need). The Acquisition program manager is the capability developer, who provides the solution to the problem (the enhanced capability).
- S&T is not on that primary path to the end users, but off to the side. If we don't find an on-ramp to that path, our efforts can have no effect on end users.
- To find that "on-ramp," we must understand the Acquisition program manager's strategies and plans, and form a partnership (perhaps via membership on an Acquisition program IPT). Such a partnership is codified in a Technology Transition Agreement (TTA), defining the enabling products which S&T will provide and defining the Acquisition program's use of those products to develop the enhanced end-user capability.
- Note that the enhancement of an end-user capability does not necessarily require that S&T develop a materiel solution (or part of it). The next slide describes the many non-materiel elements of a capability.

Q: What constitutes a “Capability”?
A: DOTMLPF-RGS

S&T primarily supports the materiel and standards domains

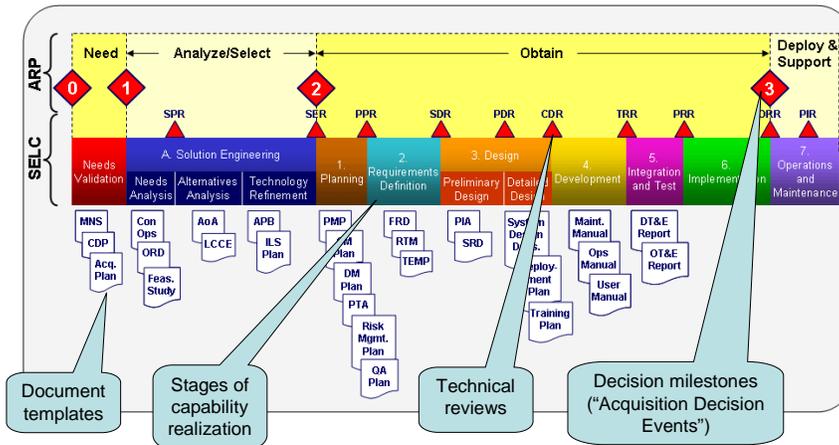
The Acquisition program must potentially address **all** capability elements

Homeland Security

6

- Not all capabilities involve materiel solutions. For example, when TSA confronted the emerging threat of liquid explosives, their solution was to limit all carry-on fluids to 3 ounces. This countermeasure didn’t involve a materiel solution, since the reaction to the threat had to be immediate and there was no adequate existing sensor system. Instead, the problem was addressed by the “D” and “T” elements of DOTMLPF-RGS: Doctrine (in the form of new standard procedures) and Training (of screeners), to restrict the amount of liquid which could be brought aboard.
- As another example of a non-materiel solution, if the desired capability is interoperable communications among local first responders, the governmental solution may involve Standards (to govern interoperable communications) and Grants (to incentivize the local agencies to buy). In this example, there are materiel elements to the capability (e.g., radios), but they are provided to the end users through their independent buying decisions, not by Government development of interoperable radios.
- In short, providing a capability to end users isn’t necessarily all about widgets.

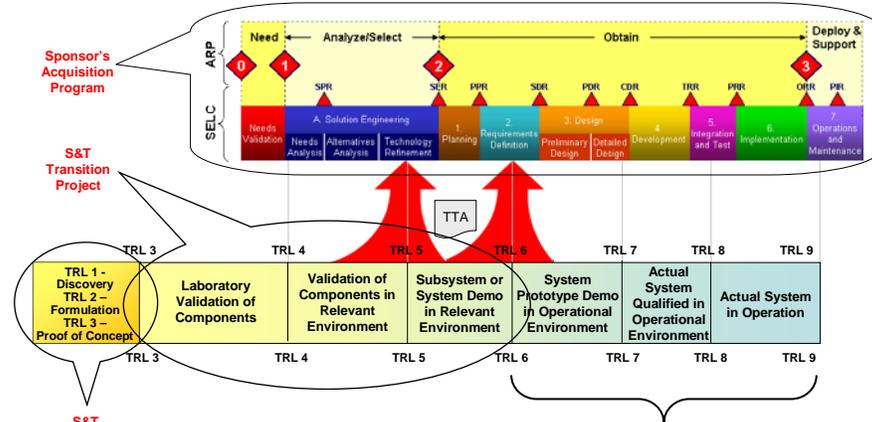
DHS's Systems Engineering Life Cycle (SELC) is the stage-gate framework for Acquisition



- The four-phase Acquisition Life Cycle, augmented by the 4-gate Acquisition Review Process, is general enough to accommodate not only new-system development of capital assets, but also other types of Acquisitions, such as service contracts, inter-agency agreements, and the DHS Strategic Sourcing Program.
- Where system development is needed, the Acquisition Life Cycle Framework can be augmented by the Systems Engineering Life Cycle (SELC), which provides a more detailed and prescriptive phase-gate framework.
- Although the SELC's details seem prescriptive, it is designed to be tailored by Acquisition program managers to suit the needs of each Acquisition program.

Slide 8

How does S&T support Acquisition?



If an S&T project develops a user system past TRL 6 without transitioning to Acquisition, it may be executing part of an Acquisition program without knowing it (a risky proposition because manufacturability and supportability will not be addressed).

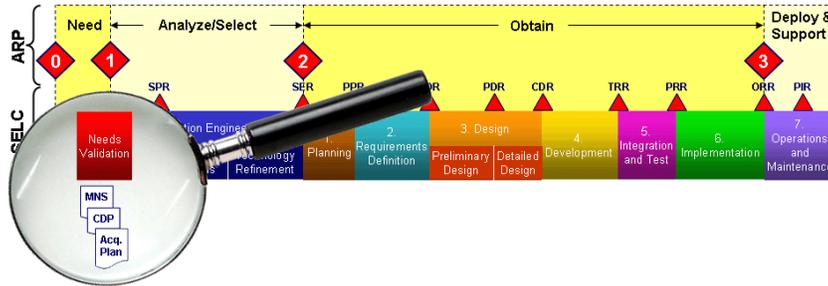


- TRL is a 9-point scale measuring technology maturity. For example, a modern cell phone is at TRL 9. In 1975, the prototype cell phone (at TRL 2) was a Ford van with a minicomputer inside and an antenna on top. Mobile phone technology matured through proof of concept (TRL 3), laboratory analyses and experiments, field experiments, etc., to the mature product you use today. There is no way, at TRL 2, to create a program plan through TRL 8 or 9, because there's too much uncertainty. So you take it a step at a time (Basic Research, then Applied Research, then Acquisition). It's all about risk reduction.
- In interpreting this diagram, don't forget the unofficial motto of DAU – "It depends." For example, the TRL at transition could be earlier than TRL 6 if the benefit is worth the added risk.
- You transition to Acquisition at TRL 6 (roughly) because (a) the risk is low enough, and (b) you haven't started final system design yet. When you're doing final system design, you need the planning and controls that the SDLC and IRP include. At TRL 7, by definition, you've demonstrated a prototype near or at planned operational system, in an operational environment. If you're that far along, the system development should be inside the Acquisition program.
- Note that there's "technology development" in the Acquisition program (CTD) phase and also in the Advanced Research project. How do they relate? "It depends." How does the new technology enter the Alternatives Analysis in CTD? Or does it? "It depends." Perhaps the technology development by S&T outside the Acquisition program is not on the critical path, and not necessary for the Acquisition (so that if it fails, the Acquisition still proceeds).
- Sponsors are responsible for Acquisition programs because 85% of the life-cycle costs are in their domain (Production, Deployment, Operations, and Support). If the Sponsor doesn't need the system badly enough to pay for these large out-year costs, there's no point in developing a system.

You don't develop a production-ready user system without entering the SDLC, and thereby submitting yourself to the IRP. Otherwise, you might end up with a system ready to ship but without any logistics system in the field. No maintenance techs, no spare parts, no manuals, no troubleshooting equipment, no user training. Also no environmental requirements. Even worse, no life-cycle funding! In other words, an Applied Research project developing a "production-ready design" of an operational system is a sneak path to the field, which is generally a bad idea (though, of course, "it depends").

Slide 9

Acquisition Program: Needs Validation

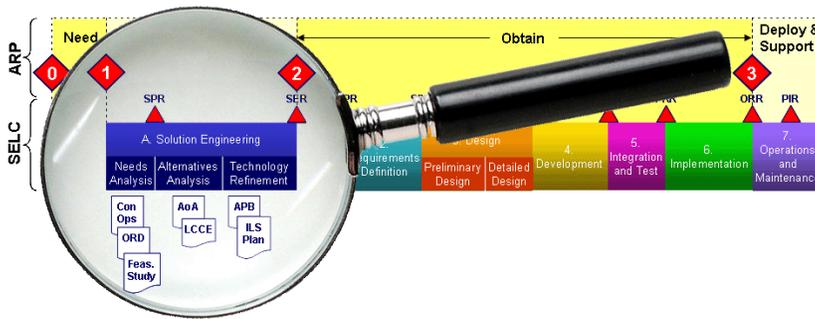


- Define or refine Mission Needs Statement
- Write Capability Development Plan
- Write preliminary Acquisition Plan
- Acquisition Decision Event 1: Approval of the mission need and the initial planning



Slide 10

Acquisition Program: Solution Engineering

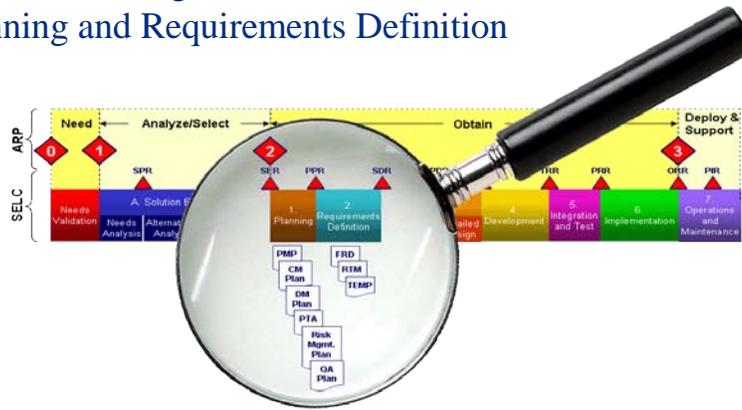


- Develop the Concept of Operations
- Assess DOTMLPF-RGS
- Develop Operational Req'ts Document
- Assess feasibility
- Analyze alternative concepts
- Select the preferred system concept
- Refine any necessary technologies
- Estimate life cycle costs
- Develop an Acquisition Plan
- Develop an Acquisition Program Baseline
- Develop an Integrated Logistics Support Plan
- Acquisition Decision Event 2: Approval to proceed with selected alternative



Slide 11

Acquisition Program: Planning and Requirements Definition



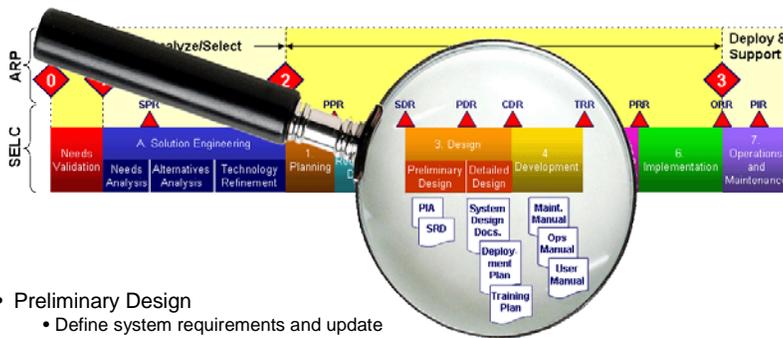
- Develop Project Management Plan
- Develop CM and DM Plans
- Conduct privacy threshold assessment
- Assess project risk and write Risk Management Plan
- Develop Quality Assurance Plan
- Develop performance requirements and flow down to subsystems and components
- Develop Functional Requirements Document
- Develop Requirements Traceability Matrix
- Develop TEMP



11

Slide 12

Acquisition Program: Design and Development



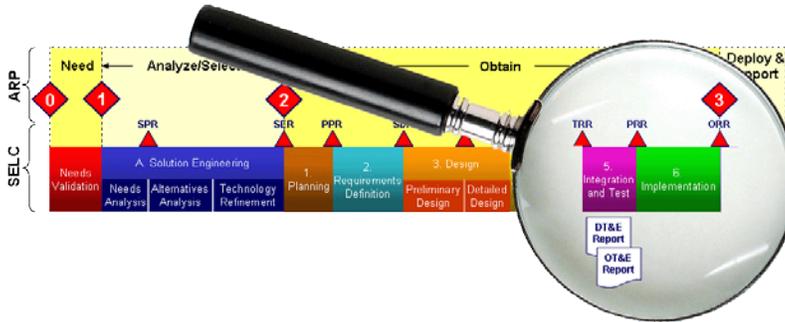
- Preliminary Design
 - Define system requirements and update the Requirements Traceability Matrix
 - Develop preliminary design
 - Conduct Preliminary Design Review (PDR)
- Detailed Design
 - Develop system design
 - Initiate Privacy Impact Assessment
 - Conduct Critical Design Review (CDR)
- Build, construct, and configure the system
- Conduct unit testing
- Develop field documentation
 - Operators manuals
 - Maintenance manuals
 - User manuals



12

Slide 13

Acquisition Program: Integration, Test, Implementation



- Verification and validation of field documentation
 - Operators manuals
 - Maintenance manuals
 - User manuals
- Developmental Test and Evaluation
- Operational Test and Evaluation
- Complete preparation of operational sites
- Transition to production
- Coordinate changes to business practices
- Conduct training
- Acquisition Decision Event 3: Approve production, deployment, support



13

Slide 14

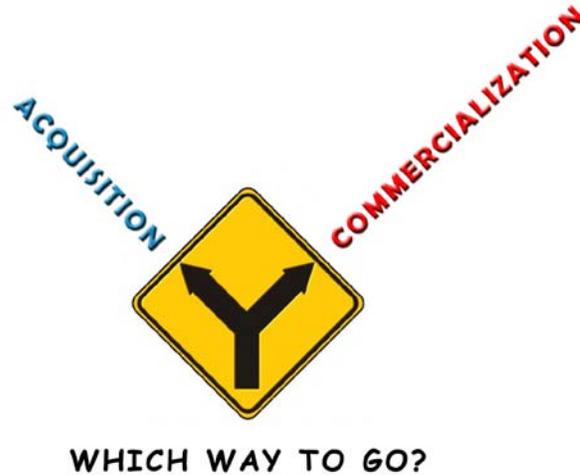
Who pays for capability development? It depends.

- In classical Big-A Acquisition, the Government pays for specialized capability development
 - Extreme examples are NASA and DoD systems
 - Limited market for a highly specialized capability, therefore no incentive for industry to fund development
 - Users are controlled by the Acquiring agency, which can therefore deploy the capability
 - Often very expensive
- However, for many DHS capability needs, classical Big-A Acquisition won't work
 - Users are not controlled by DHS, therefore make their own buying decisions
 - Commercialization is the only recourse (perhaps supported by Standards and Grants)
 - The private sector must be incentivized to develop and market the capability, and the user community must be incentivized to buy it
 - Can provide significant cost savings relative to Big-A



14

Two paths to the end user ... Big-A and Big-C



15

- Acquisition and Commercialization are very distinct processes. Accordingly, the project manager reaches a fork in the road right at the beginning of the project. Which way to go?
- Acquisition and Commercialization aren't mutually exclusive, of course, in the sense that elements of each can be blended, depending on the needs of the project. However, they are distinctly different models, and therefore it's important to understand both models before you try to combine elements of each.
- In this mini-course, whenever we mention "Acquisition," we're talking "big 'A' Acquisition, not "little 'a' acquisition." In other words, we're talking about acquiring products which don't exist, rather than procuring or purchasing products which do exist. Those who are unfamiliar with the distinction between big 'A' Acquisition and little 'a' acquisition are referred to two other mini-courses in this series: "Acquisition" and "Procurement Requisitions."
- We will also use the terms "product" and "system" interchangeably.

The two paths are different in almost every detail

Acquisition

A **government contractor** executes design, development, and production, driven by **DHS requirements**, using **DHS funding**, under **contract** to DHS. The product is then **deployed to captive users**. Product unit price is determined by **cost-based** pricing. The contractor's customer is **DHS**, not the end-user community.

Commercialization

A **private-sector enterprise** executes design, development, and production, driven by **market requirements**, using **private funding**, assisted by DHS technology **licenses, standards, and grants** if appropriate. The product is then **marketed and sold as COTS directly to end users**. Product unit price is determined by **market-based** pricing. The vendor's customer is the **end-user community**, which may or may not be in DHS.

16

- Although the two paths are extraordinarily different, they are often confused. Let's highlight the differences.
- Who develops the product?
 - In Acquisition, the developer is a government contractor (often called a prime contractor or a system integrator to make clear their responsibility for the total product or system.)
 - In Commercialization, the developer is a private-sector enterprise.
- Where do the requirements come from?
 - In Acquisition, the government specifies the requirements, based on information from its captive end users.
 - In Commercialization, the developer determines the requirements from the marketplace. The government may assert that it knows the marketplace requirements, but the developer is unlikely to invest scarce resources until they have at least validated those requirements.
- Where does the funding come from?
 - In Acquisition, from the government.
 - In Commercialization, from the developer.
- What are the formal, legal agreements between the Government and the developer?
 - In Acquisition, the relationship is governed by contracts.
 - In Commercialization, the relationship may require no legal agreements, or it may require licenses, CRADAs (Cooperative R&D Agreements), or Memoranda of Understanding.
- What are the channels by which the products reach the end users?
 - In Acquisition, by deployment to captive end users.
 - In Commercialization, by sales channels such as catalog sales, e-commerce, or direct sales. The product is referred to as COTS (Commercial Off-the-Shelf), implying that it is readily available for sale.

(Notes continued below next slide)

Highlighting the differences ...

Typically ...

	Acquisition	Commercialization
Product type	Custom	COTS
Primary users	Federal agency	State, local, private sector
Primary channel to users	Deployment	Sales
Designer & manufacturer	Gov't contractor	Private sector
Formal agreements	Contracts	Licenses, CRADAs, or none
Developer's primary customer	DHS	Marketplace
Design funder and owner	DHS	Private sector
Pricing	Cost-based	Market-based
Standards development	Possible	Likely
Grants	None	If needed

The bottom line ...

DHS relationship to developer	Control	Influence
--------------------------------------	----------------	------------------

17

(Notes continued from previous slide)

- How is the unit price determined?
 - In Acquisition, by a cost-type contract specifying a price determined by the cost of goods sold marked up by a fixed percentage.
 - In Commercialization, by price-based pricing, sometimes called market-based pricing, which means that the vendor charges what the market will bear. The market price is conventionally determined by a combination of a product's value, its manufacturing cost, and the competitive situation.
- Who does the developer consider to be their customer?
 - In Acquisition, the developer's customer is the government agency with which they have contracted.
 - In Commercialization, the developer's customer is the marketplace.

The fundamental difference between the two approaches is the question of who has control. Acquisition allows total control by the government, because the government is paying the bills. In contrast, the best the government can hope for in Commercialization is to influence the private sector, by informing them of the market and perhaps by judicious use of standards and grants programs.

How to choose between Commercialization and Acquisition?

It's all about control (or lack of it)

- **How much control do you need?**

- If the private sector can't be influenced to fund product development, or
- If DHS can't wait for the private sector to develop the product, then

Acquisition is necessary to force product development

- **How much control can you have?**

- If DHS can't afford to fund product development, manufacturing, and deployment, or
- If DHS has no authority over the users, then

Commercialization is necessary to get the product to the users

18

- The choice between Acquisition and Commercialization may boil down to two questions of control:
 - How much control is needed? (Perhaps none, if the private sector can be influenced to commercialize the product in a timely manner.)
 - How much control is achievable? (Perhaps none, if the end users are not under the authority of a DHS agency, and therefore make their own buying decisions.)
- Note that the ultimate unit price of the product will be price-based if commercialized and cost-based if acquired under contract. One can expect that market-based pricing will be higher than a cost-based pricing, because the vendor will recover the R&D costs in the market-based price of the product.
- So if the ultimate users are in a DHS agency, the choice may very well be between (a) a higher up-front cost and a lower unit purchase price (in an Acquisition program), or (b) a lower up-front cost and a higher purchase price (in a Commercialization program).
- In short, if the users are in a DHS agency, the choice may be “Pay me now or pay me later.” If indeed both the Acquisition and Commercialization paths are feasible for the desired product, total cost of ownership should be considered as a significant factor in the decision.

Two interlocking processes ...

- Every private-sector enterprise may have their own product development process.
- DHS's goal is to influence the private sector to use their process to develop a product satisfying a capability need.
- To do that effectively, DHS needs its own process for Commercialization, which is a "tailored version of the Acquisition framework"



19

- Let's be clear that we're talking about two interlocking processes here:
 1. Each private sector enterprise has its own product development process. Of course, S&T does not execute *this* process, and cannot specify it or control it, but needs to understand it in order to influence its outcome.
 2. S&T has its own Technology Commercialization process. The private sector will not execute any part of *our* process, but will need to understand certain aspects of it in order for S&T to be able to influence the private sector. For example, if S&T asserts that there is a strong market for a new product satisfying certain requirements, the credibility of this assertion may depend on the private sector's visibility into how the market size and the requirements were determined.
- This mini-course will not go into detail concerning the private sector's product development process. We will touch on it, but spend most of our time talking about *our* process.

What does an industrial product-realization process look like? It's very market-focused.



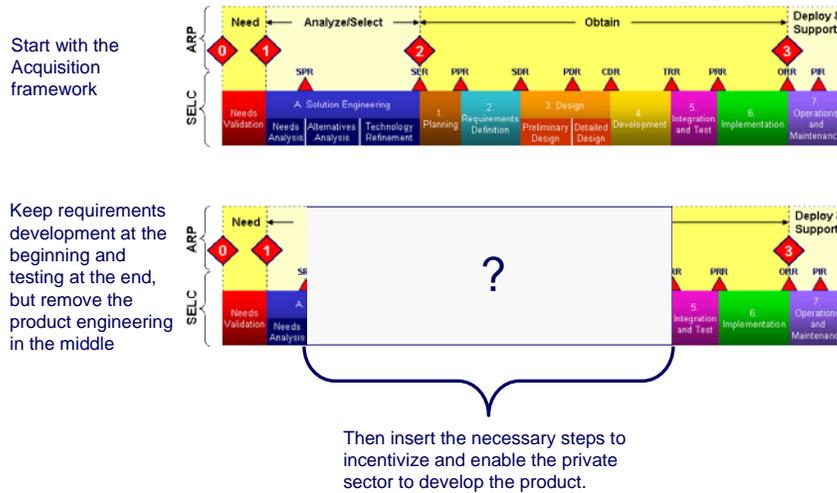
But that's "their" process. What's "our" process?

20

- Most industrial product-development processes are structured as phase-gate frameworks, since the phase-gate paradigm is the best way to organize a series of activities with periodic event-driven management reviews.
- The product-development process depicted here is a top-level description of a detailed product-development process used by S&T's Chief Commercialization Officer, Tom Cellucci, when he was a CEO and later a management consultant in the private sector.
- This phase-gate process uses a different vocabulary than any of S&T's processes, including terms such as "value proposition," "marketing," "competitive analysis," "price points," and "sales." One difficulty faced by S&T project managers of Commercialization projects is bridging the communications gap between the typical S&T technology-focused terms and the private sector's product-focused terms.
 - S&T's technology focus reveals itself in the use of terms (such as Technology Readiness Levels) which are generally unknown in the private sector. If you plan to partner with the commercial sector, you've got to learn their language, because (unlike government contractors) they won't learn yours.

Slide 21

What's "our" commercialization process? It's a tailored version of Acquisition



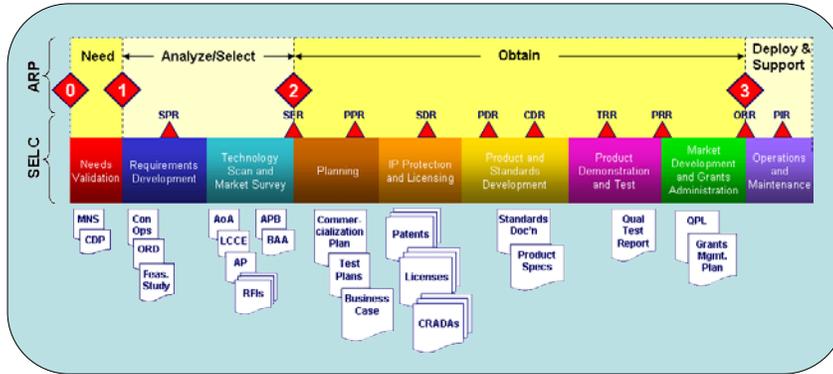
21

- S&T has developed a phase-gate process to govern Technology Commercialization, as a way of providing guidance to project managers as they navigate unfamiliar waters.
- S&T has discovered no analogous process anywhere else, because no other government agency have a proven requirements-driven process to influence the private sector to develop a new product for a specific set of users.
- This process contains elements of the commercialization process used by the Offices of Research and Technology Application (ORTAs) in DHS's National Laboratories to manage technology transfer to the private sector. However, the goal of the ORTAs is simply to transfer the technology to private-sector partners for whatever commercial purpose the private sector chooses, regardless of any connection with the Laboratory's mission. In contrast, the purpose of S&T's Technology Commercialization process is mission-driven, specifically to fill capability gaps relating to homeland security. This objective is much more difficult.
- Accordingly, this process cannot be said to be proven, but is offered as a prototype process to be used and improved.

The process is documented on S&T's RDT&E web site, a disk-based web on the S&T Shared drive. Find the file "index.htm" in the folder "RDT&E Process Website" and double-click it to reach the home page. Then click on "Transition" in the main graphic, and then on "Technology Commercialization," and you'll see the phase-gate graphic reproduced in this slide.

Slide 22

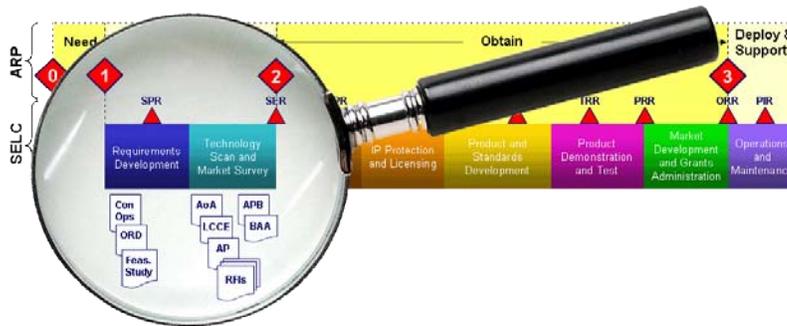
Commercialization: Here's what it might look like



Now we'll step through the stages of the tailored SELC

Slide 23

Commercialization Program: Requirements, Technology, and the Marketplace

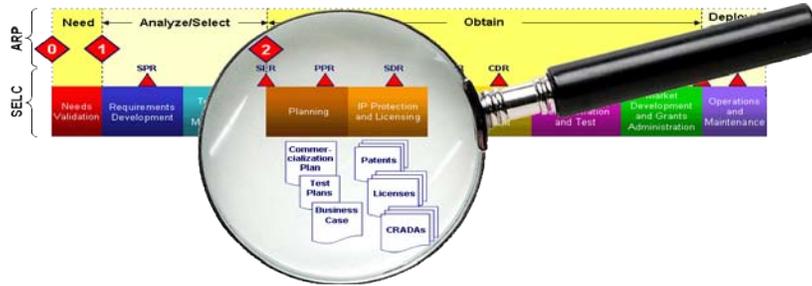


- Define the problem by documenting a ConOps and ORD
- Assess feasibility to assure that the ORD is achievable by at least one conceptual solution
- Publish the ORD and an assessment of the potential available market, to spark private-sector interest
- Conduct a technology scan and market survey to identify candidate technologies and sources
- Augment the survey with Requests for Information and use of BAAs if necessary
- Assess alternative approaches and document in an Analysis of Alternatives



Slide 24

Commercialization Program: Planning and IP

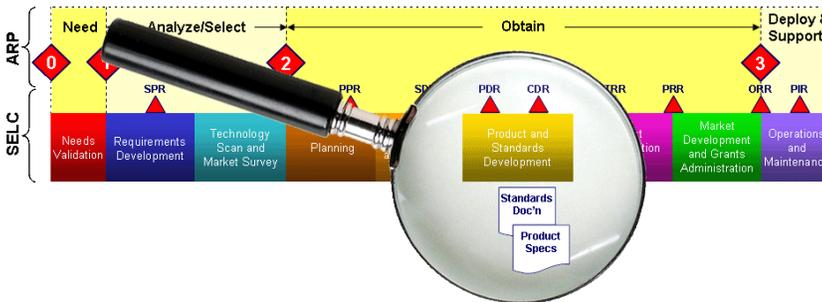


- Create a Commercialization Plan to identify and document all steps necessary to cause the product to be brought to market, including necessary standards, grants, and regulations
- Create a straw Business Case to assess the market attractiveness to the private sector
- Create test plans to document how product compliance with requirements and standards will be assured
- Protect any Government intellectual property which will be transferred to the private sector
- Implement Cooperative Research and Development Agreements (CRADAs) with industry as necessary



Slide 25

Commercialization Program: Product & Standards Development

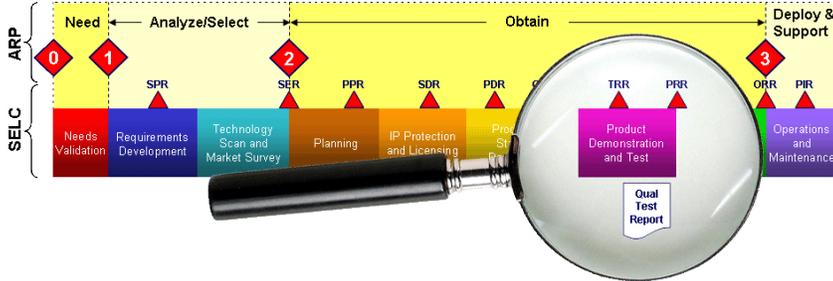


- The product is developed by the private-sector partner(s)
- Any oversight by DHS is negotiated with the private sector for mutual benefit, including rigorous reviews if prescribed by a CRADA
- New standards are developed by the DHS Standards organization, as necessary to administer downstream grants programs or to facilitate market penetration by the private-sector partner



Slide 26

Commercialization Program: Product Demonstration and Test

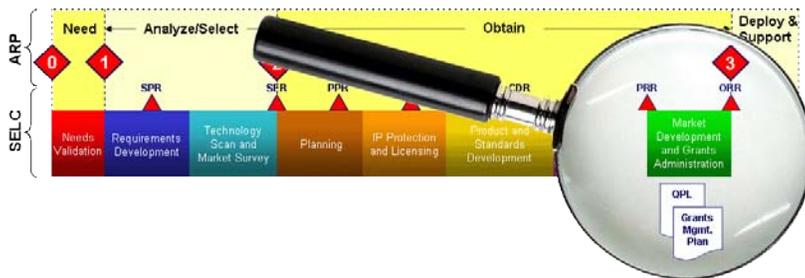


- Conduct product qualification testing or review third-party testing in accordance with the test plan, verifying product compliance with standards and with the ORD as a prerequisite for adding the product to the Authorized Equipment List (AEL) and the SECURE website
- Feed back to vendor any findings for product improvement



Slide 27

Commercialization Program: Market Development & Grants Administration



- Vendor's marketing and sales department markets the product
- DHS adds the product to the Authorized Equipment List and to the SECURE website to publicize that the product has passed DHS testing and quality standards
- DHS administers any grant programs which were part of the Commercialization Plan



Summary

- Acquisition and Commercialization are two methods to provide capabilities to users.
- Commercialization can be considered as a highly tailored version of Acquisition.
- Acquisition is characterized by control; commercialization is characterized by influence.
- Acquisition is generally required where systems are big and the market is small, or where the requirements are too specialized for the commercial sector to risk its investment capital.
- Acquisition and Commercialization are both managed by a sponsoring DHS Component which represents the users. S&T can affect the end users only indirectly.
- Commercialization may require the use of Standards, Grants (the carrot), and/or Regulations (the stick).



Additional information ...

DHS S&T Commercialization Office

The U.S. Department of Homeland Security (DHS), Science and Technology (S&T) Directorate's commercialization efforts are headed by the Commercialization Office which was officially established in October 2008. The mission of the Commercialization Office is to develop and execute programs and processes that identify, evaluate and commercialize widely-distributed products or services that meet the detailed operational requirements of DHS's operating components, first responder community, critical infrastructure/key resources (CIKR) owners and operators and other Department users. Managing and enhancing DHS S&T's outreach effort with the private sector to establish and foster mutually-beneficial working relationships leading to the fielding of technologies to secure the Nation is a primary day-to-day function of the Commercialization Office.

The SECURE Program – one of the Commercialization Office's innovative public-private partnerships enables the rapid, cost-effective and efficient development of products and services to protect the Homeland at the benefit of the taxpayers, private sector and DHS. The goal of the SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) Program is to leverage the resources of the private sector to develop solutions aligned with (and tested against) DHS generated and vetted detailed operational requirements using the private sector's experience and resources. DHS stakeholders can then make better-informed decisions on products or services specifically aligned to their requirements.
(See http://www.dhs.gov/xres/programs/gc_1211996620526.shtm)

COMMERCIALIZATION OFFICE RESOURCES

In order to facilitate outreach to the private sector and improve communications, the Commercialization Office has published a number of materials, including briefs, books and articles that outline the major activities of the Commercialization Office and provide readers with easy-to-understand guides for requirements development and the recently developed and implemented DHS commercialization process. The Commercialization Office also reaches out to businesses of all kinds – disadvantaged, small, medium and large – about opportunities that exist for partnership. The Commercialization Office makes these resources available to all who are interested. Please visit our website at http://www.dhs.gov/xabout/structure/gc_1234194479267.shtm.

Requirements Development Resources The Commercialization Office has published three popular books to assist in the development of detailed operational requirements ["Requirements Development Guide" (April 2008), *Developing Operational Requirements* (May 2008), and "Developing Operational Requirements, Version 2" (November 2008)]. These books serve as useful resources to explain the critical role of detailed requirements in the cost-effective and efficient development of products and services.

Commercialization Office Articles The Commercialization Office has published over 25 articles and a compilation of works ["Harnessing the Valuable Experiences and Resources of the Private Sector for the Public Good," (February 2009)] written at the request of the private sector to inform the public of new opportunities and ways to work with DHS. These articles inform readers about processes and the benefits of fostering a mutually beneficial partnership with DHS. Article topics include the critical role of requirements, focus on small and disadvantaged businesses, global outreach efforts and potential available markets.

Other Resources In addition, the Commercialization Office has made available a number of presentations, program concepts-of-operations and a product realization chart that correlates terminology used by both the public and private sector to delineate how science, technology development and product development are related to basic research, innovation and transition using a Technology Readiness Level (TRL) "backbone."

Feedback Welcomed! For more information on how to get involved in programs like SECURE or to provide feedback to the Commercialization Office, please send an e-mail to sandt_commercialization@hq.dhs.gov.



Homeland Security

Appendix K: Creating Change to Drive Results (Brief)

Slide 1

Creating Change to Drive Results

A journey into creating a “Commercialization Mindset” at DHS



April 2009

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
Department of Homeland Security
Email: Thomas.Cellucci@dhs.gov

Slide 2

Discussion Guide

- Change Ain't Easy
- Why Commercialization? Commercialization Office?
- It All Starts with a Plan: OSTs and the “Four Pillars”
- Top-Down and Bottom-Up plus the “Tough Middle”
- If You Can't Measure It – You Can't Manage It
- Let Others Take the Credit: Transferring Ownership
- Innovate and Automate: Using Technology as a Force Multiplier
- Glance in the Rearview Mirror but Spend Most of Your Time Looking through the Windshield
- Summary
- Open Discussion



Slide 3

Change Ain't Easy

“The art of progress is to preserve order amid change and to preserve change amid order.”
~Alfred North Whitehead



“Those who expect moments of change to be comfortable and free of conflict have not learned their history.”
~Joan Wallach Scott

“If you want to make enemies, try to change something.”
~ Woodrow Wilson



Slide 4

Why a Commercialization Office?

S&T Commercialization Office -- Four Major Activities Creating and Demonstrating Value

Parameter	Requirements Development Initiative	Commercialization Process	SECURE Program	S&T Private Sector Outreach
1) Increases speed-of-execution of DHS programs/projects	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2) DHS and its stakeholders receive products more closely aligned to specific requirements/needs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3) Increases effective and efficient communication	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4) End users can make informed purchasing decisions	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5) Large savings of cost and time for DHS and its stakeholders	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6) Increases goodwill between taxpayers, private sector and DHS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7) Fosters more opportunities for small, medium and large businesses	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8) Large taxpayer savings	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9) Possible product “spin-offs” can aid other commercial markets	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10) Promotes open and fair competition	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Return-on-DHS Investment is LARGE!

Why SECURE Program

•Multi-Use

- Provides private sector, in an open and transparent way, with what they need most - - Business Opportunities
- Provides assurance to DHS, First Responders and private sector users (like CI/KR) that products/services perform as prescribed (and provides vehicle for First Responders, CI/KR owners and operators to voice their requirements)
- Augments the value of the SAFETY Act

•Saves Money

- Private Sector uses its own resources to develop products and services to the benefit of the taxpayer and the Federal Government

•Creates Jobs

- Detailed articulation of requirements coupled with funded large, potential available markets yield OPPORTUNITY that yields Job Creation (it's better to teach a person to fish than to give them a fish)
- Enables small firms with innovative technologies to partner with larger firms, VCs and angel investors because of the credibility of having government show detailed requirements with associated market potential (instead of just their own business plans).

•Efficient Use of Government Funds

- Articulating detailed requirements saves time and money. It is better for Government to spend funds to procure products or services that are available for sale and rigorously tested compared to spending money and time to develop new solutions for ill-defined problems.

SECURE Program Benefit Analysis

“Win-Win-Win”

Taxpayers	Private Sector	Public Sector
1. Citizens are better protected by DHS personnel using mission critical products	1. Save significant time and money on market and business development activities	1. Improved understanding and communication of needs
2. Tax savings realized through Private Sector investment in DHS	2. Firms can genuinely contribute to the security of the Nation	2. Cost-effective and rapid product development process saves resources
3. Positive economic growth for American economy	3. Successful products share in the “imprimatur of DHS”; providing assurance that products really work	3. Monies can be allocated to perform greater number of essential tasks
4. Possible product “spin-offs” can aid other commercial markets	4. Significant business opportunities with sizeable DHS and DHS ancillary markets	4. End users receive products aligned to specific needs
5. Customers ultimately benefit from COTS produced within the Free Market System – more cost effective and efficient product development	5. Commercialization opportunities for small, medium and large business	5. End users can make informed purchasing decisions with tight budgets

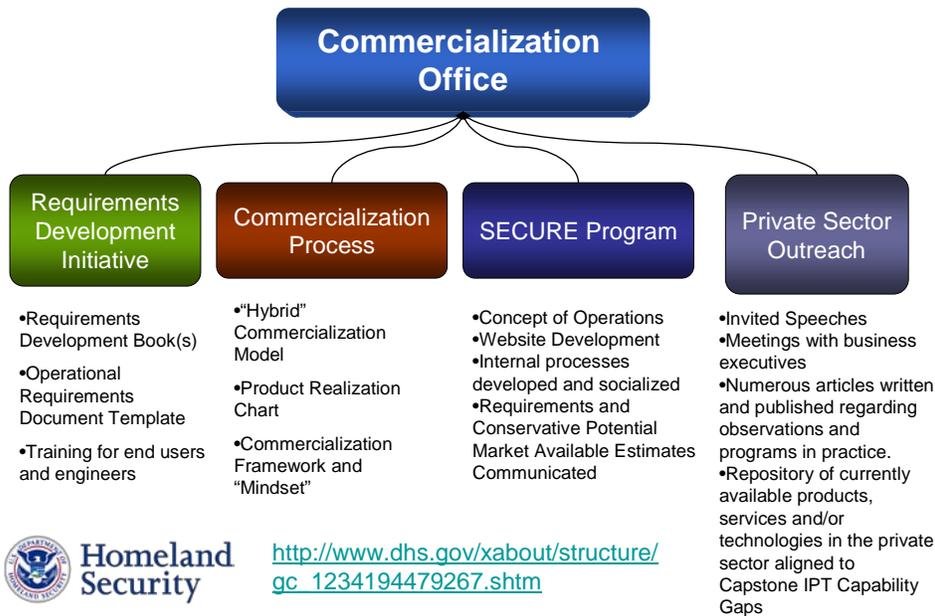
Let's Make it Happen

Commercialization Office Major Activities

Potential Benefits

<p>Requirements Development Initiative enables easy-to-use guidelines for articulating detailed operational requirements used throughout the Department to enhance internal and external communications for program/project development and execution, procurement and private sector outreach programs.</p>	<p>Net Impact: Savings of >\$2.5 Billion annually in DHS resources</p>
<p>S&T Commercialization Process ensures the cost-effective and efficient development of products/services for DHS, First Responders, and Critical Infrastructure/Key Resources owners with the aid of the private sector's resources.</p>	<p>Net Impact: When implemented across DHS, conservative savings in current and opportunity costs >\$10 Billion annually.</p>
<p>SECURE Program is an innovative public-private partnership in which DHS relays detailed operational requirements and a conservative estimate of potential available markets for a given need in exchange for the private sector to develop widely distributed product/service at their own expense.</p>	<p>Net Impact: To date, over \$261 Million has been conservatively invested in DHS projects for the SECURE Program pilot.</p>
<p>S&T Private Sector Outreach is a concerted effort to engage the private sector in understanding DHS detailed needs and establish a large repository of technologies/products/services aligned with DHS needs.</p>	<p>Net Impact: Savings of >\$350 Million in S&T Budget and opportunity costs.</p>

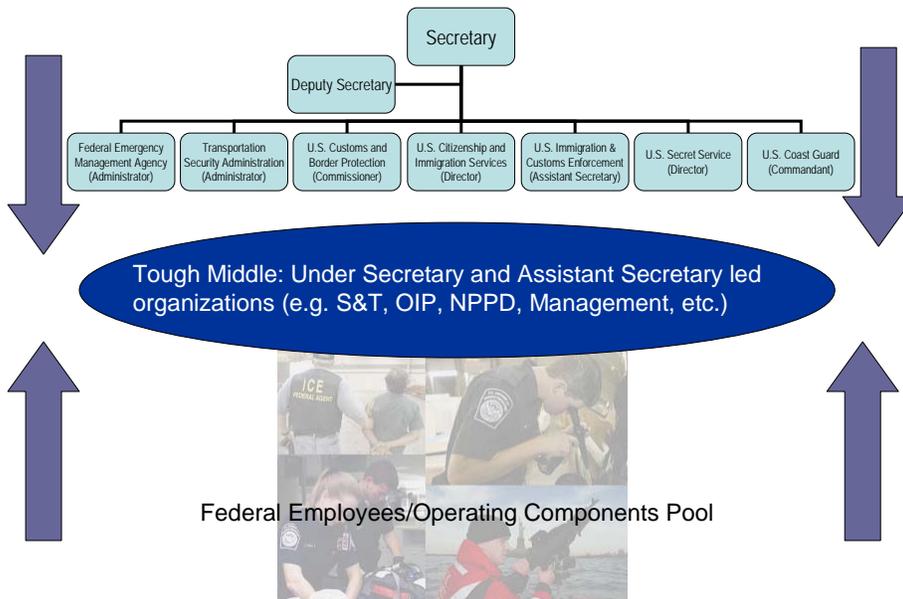
Commercialization Office: Major Activities



It All Starts with a Plan: Objectives, Strategies and Tactics

<p>Objectives</p> <ol style="list-style-type: none"> 1. Create a "Commercialization Mindset" throughout DHS by enacting Management Directive(s) consistent with our Commercialization Process by December 2009. 2. Enter into agreements/contracts related to a minimum of six products aligned to DHS ORDs by December 31, 2008. 3. Post a minimum of ten DHS sponsored ORDs (and accompanying market estimates) on SECURE website by March 2009. 	<p>Strategies</p> <ol style="list-style-type: none"> 1. Develop "top-down" and "bottom-up" awareness and use of commercialization processes through briefings to Senior Executives, S&T Corporate Board and Transition and Program Managers 2. Continue to meet with S2/G-7 Senior leadership to receive projects/ideas for possible commercialization throughout the Department 3. Work with Private Sector Office to expand outreach to Private Sector entities and develop policies for commercialization initiatives 4. Expand exposure of SECURE Program on DHS.gov through media, speaking appearances, press releases, and other PR and marketing communications initiatives. 5. Develop internal processes to expedite the use of SECURE Program.
<p>Tactical Elements</p> <ol style="list-style-type: none"> 1. Distribute <i>Requirements Development Guide</i> and <i>Developing Operational Requirements</i> to personnel in and associated with DHS – e.g. Operating Components, First Responders and S&T with assistance from Office of Public Affairs/Corporate Communications (on-going) 2. Conduct small group training for S&T Division Heads, Transition Managers and Program Managers on requirements development and the context in which requirements fit into product development and commercialization lifecycles (due by October 31, 2008) 3. Assist in creation of a directive for S&T staff to receive training on requirements development (by March 2009) 4. Assist in creation of a directive for all projects resulting in end-user products to require ORDs before appropriation of monies by Jan 31, 2009 5. Assist in creation of a directive outlining the "hybrid" Commercialization Process for use in DHS product development cycles by April, 2009 6. Inform Members of Congress and Senate with updates on commercialization initiative progress on a quarterly basis (on-going) 7. Provide regular updates to Deputy Secretary (S2) and G-7 on commercialization initiative progress on a monthly basis (on-going) 8. Develop and implement a mechanism to inform and make available to S&T personnel company overview documents received as part of Private Sector outreach efforts (due by July 31, 2008) 9. Develop process by which conservative estimates of potential available markets are generated (due by September 30, 2008) 10. Develop process by which Operational Requirements Document are reviewed and placed on SECURE website (due by September 30, 2008) 11. Develop process by which third party independent T&E is evaluated and results reported on SECURE website (due by October 31, 2008) 12. Work with Office of Public Affairs (OPA) to place articles in more media outlets, post "Opportunities for the Private Sector" brief online, and expand content of SECURE website (due by August 31, 2008) 13. Collaborate with Operating Components and First Responders to write ORDs for problems not addressed by current S&T projects. (on-going) 14. Monitor progress against goals and update OST (on-going) 	

Top-Down, Bottom-Up Socialization



Public Vs. Private Sector

Typical Drivers and Motivators

Public Sector

- Advancing Public Good
- Fulfilling Needs of Stakeholders/ Constituents
- Following clear processes and methods
- Power of the Purse Strings
- Strive for Perfection
- Job Security
- Commitments/Obligations/ Expenditures

Private Sector

- Sales Opportunities
- Market Development
- Profit Margins
- Raising capital
- Increasing shareholder value
- Efficiency and Cost-Effectiveness
- Speed of Execution
- Results/Output

Challenge: Enabling and fostering common goals to facilitate mutually beneficial programs

Critical Role of Metrics

- Number of Products/Services Developed and Deployed
- Number of Technologies Transitioned
- Return on Investment
- Taxpayer Money Saved
- Speed of Execution – ORD draft, review process and development of product/service

“If you can’t measure it, you can’t manage it”



Let Others Take the Credit

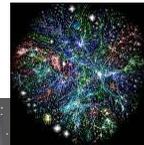
- Success has a thousand fathers
- SECURE Pilot “Primed the Pump”
- Headquarters takes ownership of ORDs
- People want to be productive and efficient
- Imitation is the sincerest form of flattery



Innovate and Automate

Evolution of Change: DHS Providing Better Information about its Needs

DoD, DoE, DHS,
DoJ, DoT, etc.



DHS **Federal Stakeholders**



Slide 15

Moving Forward

Lessons Learned

- Communicate and Iterate, Iterate and Iterate
- Strive for Excellence, Not Perfection!
- Have a back-up to the back-up of the back-up
- Expect the Unexpected
- Plan, Measure and Report
- Education is key
- Demonstrate benefits for all parties
- Put it in writing



Things to Come

- Semantic Web 3.0
- Communities of Practitioners
- Continued Outreach/Interaction with Stakeholders and Private Sector
- Leveraging new R&D opportunities with universities, national labs, regional technology consortiums, etc.

Slide 16

Summary

- Make it Easy/Keep it Simple
- Never (ever) Give Up
- Innovate
- Re-Iterate
- Contemplative-in-Action

Slide 17



Open Discussion/Questions

Slide 18



**Homeland
Security**

Appendix L: Demonstrating Efficiency Brief

Slide 1

Commercialization Office: Providing Value through Efficiency and Cost-Effectiveness



April 2009

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
Department of Homeland Security
Email: Thomas.Cellucci@dhs.gov

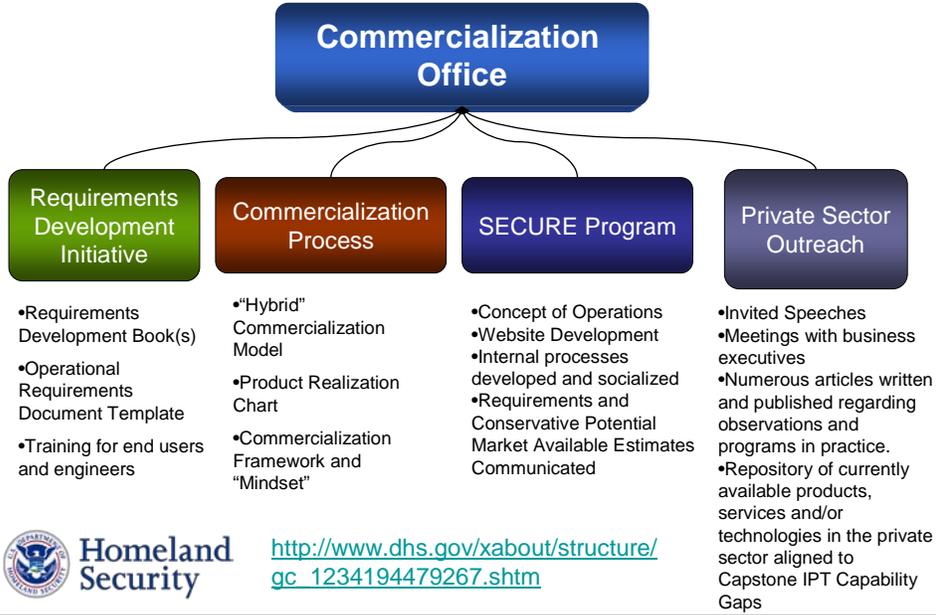
Slide 2

Discussion Guide

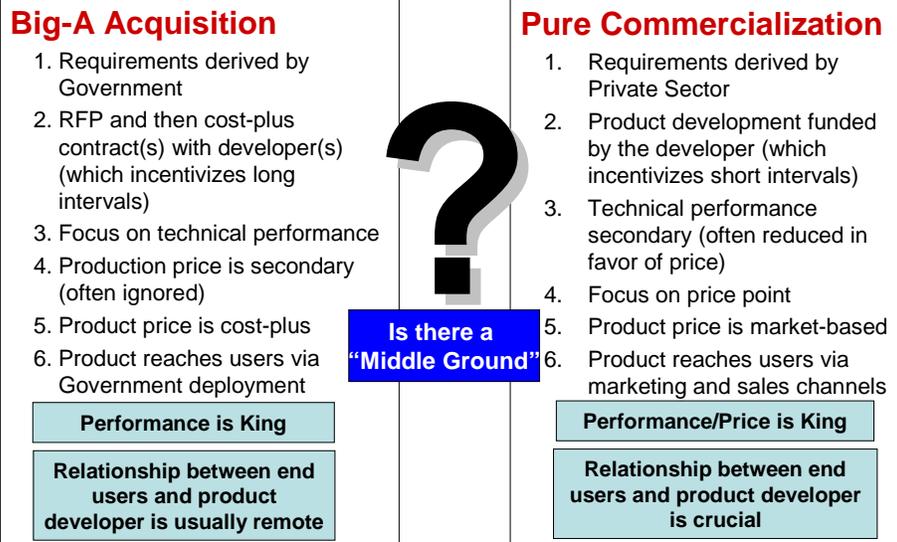
- Commercialization Office Initiatives at DHS
- New Commercialization Process
- Outreach Efforts
- SECURE Program
- Benefits for Taxpayers, DHS and Private Sector



Commercialization Office: Major Activities



Two Models for Product Realization



A New Model for Commercialization

1. Development of Operational Requirements Document (ORD)
2. Assess addressable market(s)
3. Publish ORD and market assessment on public DHS web portal, soliciting interest from potential partners
4. Execute no-cost agreement (streamlined CRADA) with multiple Private Sector entities, transferring technology (if necessary)
5. Develop supporting grants and standards as necessary
6. Assess T&E after product is developed
7. New Commercial off the Shelf (COTS) product marketed by Private Sector with DHS support

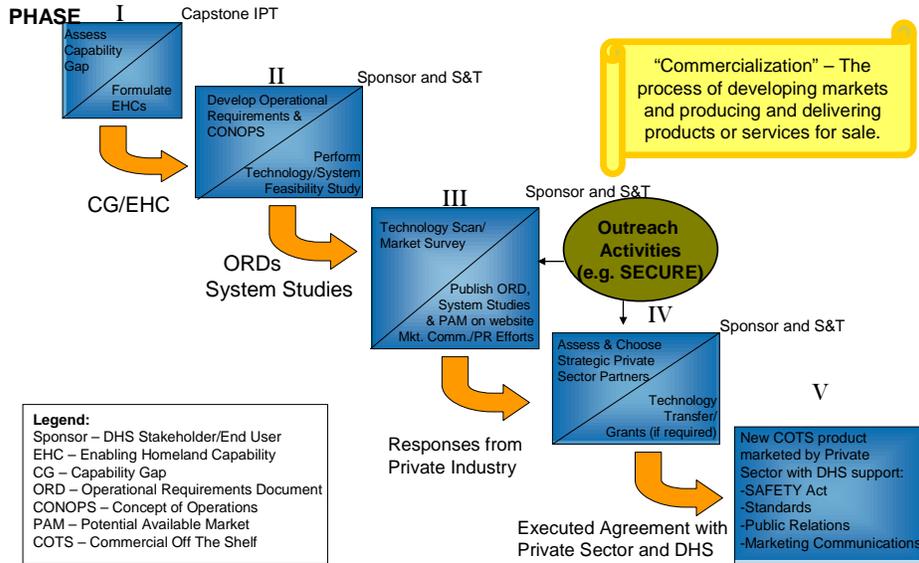
Differences from the Acquisition model:

- Primary criteria for partner selection is market penetration, agility, and performance/price ratio
- Product development is not funded by DHS
- Government involvement is limited to inherently governmental functions (e.g., Grants and Standards)



Slide 7

Commercialization Process



Slide 8

ORD: Operational Requirements Document

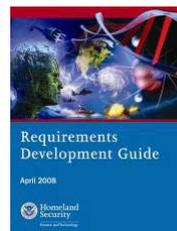
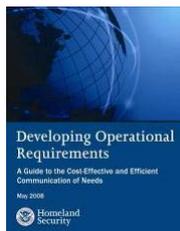
What: ORDs provide a clear definition and articulation of a given problem.

How: Training materials have been developed to assist drafting ORDs.

– *Developing Operational Requirements*, 194pp. Available online:
http://www.dhs.gov/xlibrary/assets/Developing_Operational_Requirements_Guides.pdf

When: For Use in Acquisition, Procurement, Commercialization and Outreach Programs –Any situation that dictates detailed requirements (e.g. RFQ, BAA, RFP, RFI, etc.)

Why: It's cost-effective and efficient for both DHS and all of its stakeholders.



Why SECURE Program

•Multi-Use

- Provides private sector, in an open and transparent way, with what they need most - - Business Opportunities
- Provides assurance to DHS, First Responders and private sector users (like CI/KR) that products/services perform as prescribed (and provides vehicle for First Responders, CI/KR owners and operators to voice their requirements)
- Augments the value of the SAFETY Act

•Saves Money

- Private Sector uses its own resources to develop products and services to the benefit of the taxpayer and the Federal Government

•Creates Jobs

- Detailed articulation of requirements coupled with funded large, potential available markets yield OPPORTUNITY that yields Job Creation (it's better to teach a person to fish than to give them a fish)
- Enables small firms with innovative technologies to partner with larger firms, VCs and angel investors because of the credibility of having government show detailed requirements with associated market potential (instead of just their own business plans).

•Efficient Use of Government Funds

- Articulating detailed requirements saves time and money. It is better for Government to spend funds to procure products or services that are available for sale and rigorously tested compared to spending money and time to develop new solutions for ill-defined problems.

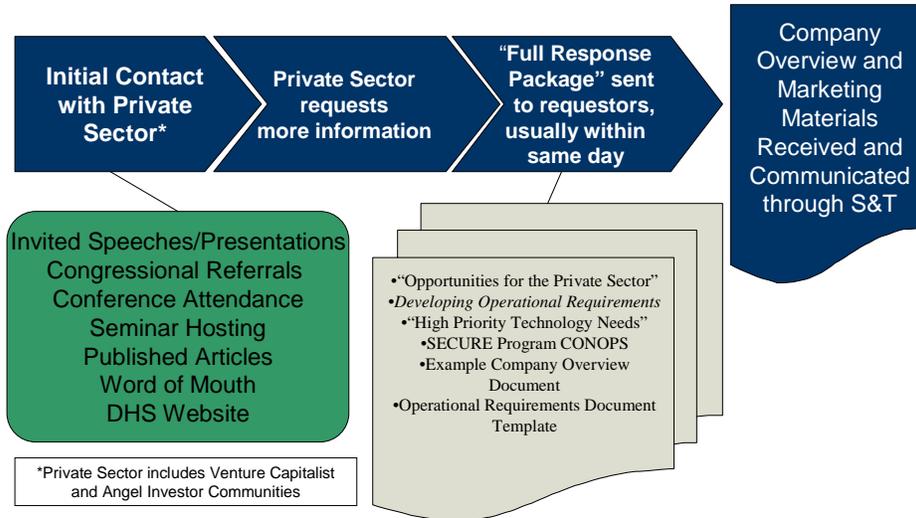
SECURE Program Benefit Analysis

“Win-Win-Win”

Taxpayers	Private Sector	Public Sector
1. Citizens are better protected by DHS personnel using mission critical products	1. Save significant time and money on market and business development activities	1. Improved understanding and communication of needs
2. Tax savings realized through Private Sector investment in DHS	2. Firms can genuinely contribute to the security of the Nation	2. Cost-effective and rapid product development process saves resources
3. Positive economic growth for American economy	3. Successful products share in the “imprimatur of DHS”; providing assurance that products really work	3. Monies can be allocated to perform greater number of essential tasks
4. Possible product “spin-offs” can aid other commercial markets	4. Significant business opportunities with sizeable DHS and DHS ancillary markets	4. End users receive products aligned to specific needs
5. Customers ultimately benefit from COTS produced within the Free Market System – more cost effective and efficient product development	5. Commercialization opportunities for small, medium and large business	5. End users can make informed purchasing decisions with tight budgets

Slide 11

Contact with the Private Sector



Slide 12

Commercialization Office - Return on Investment (ROI)

Assumptions for Conservative ROI Projections:

- > *Return on Investment* – (Gain on Investment/Cost Savings – Cost of Investment) / Cost of Investment
- > *Gain on Investment/Cost Savings* – conservative estimate of potential savings of nominally expended R&D dollars at S&T; in general, estimated savings is 75% of given/related FY09 enabling homeland capability (EHC), which is identified through Capstone IPT process
- > *SECURE Program – Cost of Investment* – 20% of Commercialization Office personnel salary + (10% Other expenses such as OGC, OPA, CCD, etc.); divided by 20 operational requirements documents (ORDs) completed and publically released in given year
- > *R&D Funds at DHS S&T* – R&D funds do not include labor or overhead (not fully burdened cost of managing program/projects/EHCs)

SECURE Program – ORD	Market Size	ROI
Blast Resistant Autonomous Video Equipment (BRAVE) ORD Requirements for a forensic camera deployed in public transportation vehicles to assist in incident cause analysis.	Over 1.5 million units	290
National Emergency Response Interoperability Framework and Resilient Communication System of Systems ORD Requirements for a system to provide interoperable communications on a national framework for remote use by first responders.	Over 2,000 units	525
Interoperable Communications Switch ORD Requirements for an interoperability switch-based communications system that provides networked communications between any number of agencies and personnel.	Over 230 units	525
Crisis Decision-Support Software ORD Requirements for a system with a user-centric approach matched with an expansive database of past decisions and a proven method to quickly reach critical decisions in high pressure environments for wide operational use.	Approx. 50,000 units	1023
Blast Mitigation of Fuel Tank Explosions ORD Requirements for an explosion suppression system to protect fuel containers. A "fuel container" ranges from fuel tanks found in vehicles, boats or trains to fuel storage tanks at airports, seaports and the neighborhood gas station.	Over 1 million units	727
Integrated Intrusion Protection ORD Requirements for an adaptable, scalable surveillance capability that provides automated, real-time protection for a wide range of operational scenarios.	Over 41,000 units	290
Predictive Modeling for Counter-Improvised Explosive Devices (IED) ORD Requirements for a system to predict the threat of an IED attack and further data fusion from law enforcement, intelligence partners and other sources to support the common operating picture.	Over 250,000 seats in US alone	870

Return on DHS Investment is LARGE when compared to Angel Investors (4x to 7x) and Venture Capitalists (5x to 20x)

Slide 13

Let's Make it Happen

Commercialization Office Major Activities

Potential Benefits

<p>Requirements Development Initiative enables easy-to-use guidelines for articulating detailed operational requirements used throughout the Department to enhance internal and external communications for program/project development and execution, procurement and private sector outreach programs.</p>	<p>Net Impact: Savings of >\$2.5 Billion annually in DHS resources</p>
<p>S&T Commercialization Process ensures the cost-effective and efficient development of products/services for DHS, First Responders, and Critical Infrastructure/Key Resources owners with the aid of the private sector's resources.</p>	<p>Net Impact: When implemented across DHS, conservative savings in current and opportunity costs >\$10 Billion annually.</p>
<p>SECURE Program is an innovative public-private partnership in which DHS relays detailed operational requirements and a conservative estimate of potential available markets for a given need in exchange for the private sector to develop widely distributed product/service at their own expense.</p>	<p>Net Impact: To date, over \$261 Million has been conservatively invested in DHS projects for the SECURE Program pilot.</p>
<p>S&T Private Sector Outreach is a concerted effort to engage the private sector in understanding DHS detailed needs and establish a large repository of technologies/products/services aligned with DHS needs.</p>	<p>Net Impact: Savings of >\$350 Million in S&T Budget and opportunity costs.</p>

Slide 14



Homeland Security

Appendix M: DHS S&T High Priority Technology Needs



High-Priority Technology Needs

May 2009



Homeland
Security

Science and Technology

Version 3.0



Homeland Security

Science and Technology

May 2009

Delivery of homeland security technological capabilities is what the DHS S&T Directorate is all about. We *know* what our customers need, and you'll find an overview of those needs in this booklet. We *don't know* where the good ideas will come from. That's why we're offering this-third edition booklet to you. Share it with your colleagues. You can also find it on the Web at www.dhs.gov.

We are delighted to speak with you anytime, anywhere, if you believe you can bring us a technology that meets a customer requirement.

Since the last edition, we've added requirements from our newly commissioned 13th Integrated Product Team devoted to state, local, tribal, and territorial first responders and emergency managers.

I hope you find this useful. Thanks for all you do to help keep the Nation safer.

A handwritten signature in black ink that reads "BI Buswell".

Bradley I. Buswell
Under Secretary (Acting)
Science and Technology Directorate
U.S. Department of Homeland Security

The S&T Capstone Transition Program

DHS S&T's Transition Program is customer-focused and output-oriented. The Directorate's near-term efforts are aligned to our DHS customers' critical needs in the form of Enabling Homeland Capabilities (EHCs), consisting of technologies that can be developed, matured, delivered, and commercialized or validated as a standard within a 3-year period.

A formalized, structured process, the DHS Transition Program aligns investments to Agency requirements and is managed by Capstone Integrated Product Teams (IPTs). These teams consist of our DHS customers and critical stakeholders and are specifically chartered to ensure that technologies are engineered and integrated into systems scheduled for delivery and made available to DHS customers. Investments are competitively selected and focus on DHS's highest-priority requirements that provide capability to DHS operating components and first responders.

With the addition of the First Responder Capstone IPT, there are now 13 Capstone IPTs in the following functional areas:

1. First Responder
2. Border Security
3. Cargo Security
4. Maritime Security
5. Cyber Security
6. Information Sharing
7. Interoperability
8. Transportation Security
9. Counter-IED
10. Chemical/Biological Defense
11. People Screening
12. Infrastructure Protection
13. Incident Management

The DHS S&T Transition Program is continuously evolving through incorporation of best practices from industry and other federal partners. As priorities change, the process is flexible enough to accommodate necessary changes while maintaining the stability of prior-year decisions.

Please note that each Capstone IPT page has block text and italic text. The block text denotes information that was presented in the previous version of this booklet. Italic text denotes new/revised information.

DHS S&T's Six Technical Divisions



The mission of the Department of Homeland Security is to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that may occur. The strategies the Science & Technology Directorate will use to accomplish those Department goals and make the Nation safer are:

The S&T Directorate's **Explosives Division** promotes the development of effective techniques to protect our citizens and our country's infrastructure against the devastating effects of explosives by seeking innovative approaches in detection and in countermeasures. It provides the concepts, science, technologies, and systems that increase protection from explosives and promotes the development of field equipment, technologies, and procedures to interdict suicide bombers, car and truck bombs, and shoulder-fired missiles before they can reach their targets.



The S&T **Chemical/Biological Division** seeks out the science needed to reduce the probability and potential consequences of a biological pathogen or a chemical attack on the Nation's civilian population, its infrastructure, or its agricultural system. The division develops and implements early detection and warning systems for attack characterization. Priorities include research and development efforts on urban monitoring, detection technologies, bioassays, a bioforensics capability, and restoration and response tools and technologies.



When making critical decisions—from evacuating civilians from a hurricane's path to preventing a terrorist attack—responders and planners need information that is relevant, accurate, and timely. S&T's **Command, Control and Interoperability Division** (CID) provides the technologies, processes, infrastructure, and mechanisms that allow these decision-makers to gather, analyze, manage, protect, and share critically needed homeland-security information, be it voice, data, or imagery.



The mission of the **Borders and Maritime Security Division** is to develop and transition technical capabilities that enhance U.S. border security without impeding commerce & travelers' flow. The Division serves as the Nation's primary shepherd of Cargo, Borders and Maritime Security science and technology with areas of responsibility that encompass all air, land and maritime borders (including U.S. ports-of-entry and inland waterways). BMD understands the technical dimension of homeland security challenges and provides customers with new and/or better options to accomplish their mission.



S&T looks at biometrics, motivation and intent, hostile intent, human factors engineering, and the social/behavioral/economic sciences to improve detection, analysis, and understanding of threats posed by individuals, groups, and radical movements. The efforts of the S&T **Human Factors/Behavioral Sciences Division** support the preparedness, response, and recovery of communities affected by catastrophic events.

The need to protect the country's 18 areas of critical infrastructure from acts of terrorism, natural disasters, and accident, is paramount, but so are state and local preparedness and response. S&T's **Infrastructure/Geophysical Division** addresses physical, cyber, and human elements of our Nation's vulnerable infrastructure, focusing on capabilities, needs, and gaps, and on known threats.



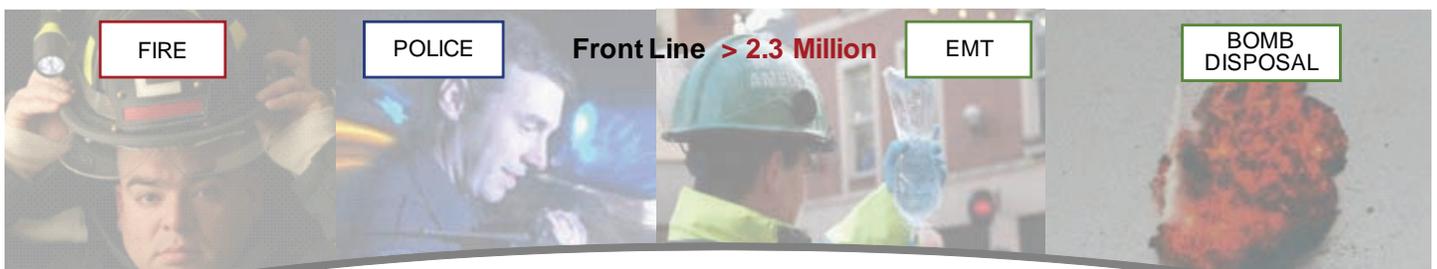
In short, when dedicated scientists, engineers, and thinkers push the boundaries of challenge, and when they are committed to the security of our Nation, they can help ensure that new mission-critical capabilities are created, knowledge is generated, and needed technologies are deployed to the right places.

DHS Customers and Customers of Our Customers

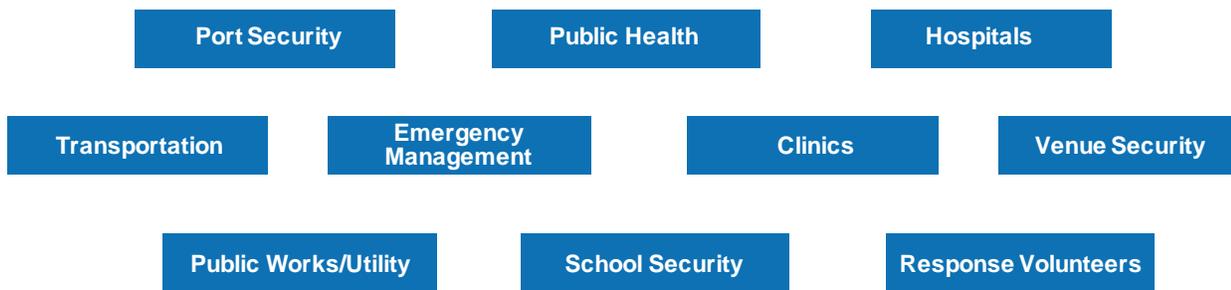
DHS S&T enables its customers—the DHS components—and their customers on the front lines, with technical capabilities to carry out their missions. Customers include state, local, and tribal entities, Border Patrol agents, Coast Guardsmen, Customs officials, Federal Air Marshals, airport baggage screeners, and first responders at the state, local, tribal and territorial levels. The responders—fire fighters, police, emergency medical technicians, and bomb disposal experts—act decisively to protect people and property, to tend to the injured, and to bring a measure of calm and clear thinking to chaotic situations. DHS S&T supports them with the tools they need to perform their jobs more efficiently, quickly, and safely, and with greater accuracy.

S&T customers, like USCG and CBP, oversee 95,000 miles of coastline, lakes, and inland waterways and 7,500 miles of the U.S. border. They safeguard 327 official ports of entry—by air, land and sea. Other customers protect the critical infrastructure that keeps our society functioning—the hospitals and public health facilities, schools, transportation systems, water supply, power plants, food supply—and the cyber backbone that underpins essential services—and much more.

Through processes like our Capstone Integrated Product Teams, S&T works with our customers in defining the capabilities they need to secure the Nation. We bring key stakeholders in the process to the table to establish a plan for getting needed capabilities into the development or acquisition pipeline so that vital needs are addressed.



Support to Front Line > 23 Million



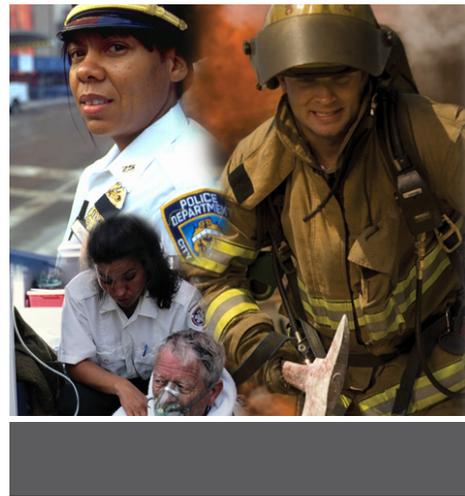
FIRST RESPONDER

DHS Lead: FEMA; Office of Intelligence and Analysis (OI&A); National Protection and Programs Directorate (NPPD)

The First Responder Capstone IPT coordinates the identification and prioritization of technology requirements and capability gaps of the Federal, state, local, territorial and tribal first responders. Identified technology solutions will be designed, tested, and assessed for usability and commercialized for the first responder community.

REPRESENTATIVE TECHNOLOGY NEEDS

- Capability to interrogate a vehicle at range and perform diagnostic and defeat procedures on explosives (Explosives Division/C-IED Capstone IPT)
- Non-lethal compliance measures for people, vehicles, vessels, or aircraft, allowing safe interdiction by law enforcement personnel (Borders and Maritime Security Division/Border Security Capstone IPT)
- Personnel-safe, handheld non-intrusive inspection devices that allow for the inspection of hidden or closed compartments (Borders and Maritime Security Division/Border Security Capstone IPT)
- Capability for law-enforcement personnel to detect and identify narcotics, chemical warfare agents, toxic industrial chemicals, explosives, and contraband materials. Improved screening and examination by non-intrusive inspection (Borders and Maritime Security Division/Cargo Security Capstone IPT)
- Capability to enhance disaster preparedness in communities (Human Factors/Behavioral Sciences/People Screening Capstone IPT)
- Respiratory protection against airborne particulate matter and poisonous gases—in particular, protective breathing equipment during the clean-up and recovery process (Chemical/Biological Division and Infrastructure and Geophysical Division/Chemical-Biological Defense Capstone IPT and Incident Management Capstone IPT)
- Capability to predict criminal and terrorist activity (Human Factors/Behavioral Sciences/People Screening Capstone IPT)
- Cost-effective training technologies for first responders depicting real-world scenarios (Infrastructure and Geophysical Division/Incident Management Capstone IPT)
- Enhanced ambulance safety and improved ambulance situational awareness and voice/data communications (Command, Control and Interoperability Division/Interoperability Capstone IPT)
- Enhanced capability to identify individuals and verify the professional credentials of individuals in both pre-planned and developing events (Human Factors/Behavioral Sciences/People Screening Capstone IPT)
- Provide emergency managers with seamless data, voice, and video information for enhanced situational awareness in major and minor crisis (Command, Control and Interoperability Division/Interoperability Capstone IPT)
- Enhanced information management capabilities to make available information more useful. In particular, the enhanced integration and intelligent prioritization of information (Command, Control and Interoperability Division/Interoperability Capstone IPT)



Randel Zeller, Director of Interagency and First Responder Programs
 Email: IAD-FirstResponder@dhs.gov





BORDER SECURITY

DHS Leads: Customs and Border Protection and Immigration and Customs Enforcement

Border security represents a myriad of challenges. Detection and identification, and, when required, apprehension and law enforcement, represent a significant portion of the DHS mission. The Border Security IPT works to prioritize functional mission needs and to identify solution space for the path to successful technology development. This leads to the development of mature technologies that support rapid, coordinated, and safe responses to anomalies and threats against the Nation and the personnel assigned to conduct the mission. The primary Federal customers for the IPT are U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE), who represent end users such as Border Patrol agents, CBP Air and Marine personnel, and ICE special agents.

REPRESENTATIVE TECHNOLOGY NEEDS

- Detection, tracking, and classifying of all threats along the terrestrial and maritime border—in particular, technologies to support tunnel detection and rugged terrain, concealing foliage, water obstacles, mountains, and other environmental constraints (Borders and Maritime Security Division)
- Personnel-safe, handheld, non-intrusive inspection device that allow the inspection of hidden or closed compartments—in particular, *the ability to find contraband and security threats (people) through steel walls. Unit must contain sensor and active source, if required, in same device. Technologies other than x-ray, gamma rays, and neutrons are desired.* (Borders and Maritime Security Division)
- Ability for law enforcement officers to assure compliance of lawful orders using non-lethal means—in particular, the ability to disable vehicles/vessels and temporarily incapacitate persons to prevent the infliction of damage or harm (Borders and Maritime Security Division)
- Improved analysis and decision-making tools that will ensure the development and implementation of border security initiatives—in particular, *a decision support effort researching automated evaluation of proposed actions through expert systems and modeling and simulation for border security. The effort is researching ways to fully integrate multiple domains, including technology, managerial, policy, organizational, political, and contextual, to enhance decision making* (Borders and Maritime Security Division)
- Non-lethal compliance measures for vehicles, vessels, or aircraft, allowing safe interdiction by law enforcement personnel—in particular, *the use of a compact, tuned, and focused energy system to shut down or disrupt normal vehicle operation while leaving the breaking and steering unaffected* (Borders and Maritime Security Division)

Anh Duong, Division Head, Borders and Maritime Security

Email: SandT-BordersMaritime@dhs.gov



CARGO SECURITY

DHS Lead: Customs and Border Protection

The Cargo Security IPT provides guidance for the development of technology and the accumulation of knowledge that address the difficult issues associated with managing the Nation's supply chain of incoming and outgoing goods and commodities. This IPT focuses on the operational needs of U.S. Customs and Border Protection (CBP) and the Transportation Security Administration (TSA), with DHS Policy and the U.S. Coast Guard as high-level stakeholders. The user community associated with the technologies and knowledge products developed in this IPT area consists of CBP Office of Field Operations (OFO) Officers, TSA Officers, and the private-sector shipping companies. The Cargo Security IPT is concerned with the full spectrum of requirements associated with improved and reliable scanning of cargo and conveyances for unauthorized items and personnel, associated information management, intrusion detection, and other anomalies while maintaining the steady flow of commerce. The IPT takes a system-of-systems, integrated approach toward development of technological solutions that will satisfy clearly stated mission requirements.

REPRESENTATIVE TECHNOLOGY NEEDS

- Improved screening and examination by non-intrusive inspection—in particular, the ability to detect or identify contraband items (for example, drugs, money, illegal firearms), threat materials, or stowaways; improve penetration, resolution, throughput, contrast sensitivity, reliability, mobility, and interoperability; and integrate with future Automated Target Recognition capability (Borders and Maritime Security Division)
- Increased information fusion, anomaly detection, Automatic Target Recognition—in particular, automated imagery detection capability for anomalous content (e.g., stowaways, hidden compartments, contraband), and the ability to detect anomalous patterns in shipping data (Borders and Maritime Security Division)
- Capability to screen 100 percent of air cargo—in particular, *the use of next generation non-intrusive inspection systems to detect and identify contraband items or stowaways without disrupting the flow of commerce* (Borders and Maritime Security Division)
- Track domestic high-threat cargo—in particular, the ability to track DHS-designated Toxic Inhalation Hazardous (TIH) cargos in domestic transit (Borders and Maritime Security Division)
- Positively identify cargo and detect intrusion or unauthorized access—in particular, in containerized, palletized, parcel, or bulk/break-bulk maritime and air cargo (Borders and Maritime Security Division)
- Reliable container seal security/detect intrusion devices—in particular, *combining six-sided container/conveyance intrusion detection with the ability to sense the presence of harmful or hazardous materials (e.g., explosives, RADNUC, Chemical, and Biological agents)* (Borders and Maritime Security Division)

Anh Duong, Division Head, Borders and Maritime Security

Email: SandT-BordersMaritime@dhs.gov





MARITIME SECURITY

DHS Lead: United States Coast Guard

The U.S. maritime environment is a great expanse, requiring several DHS operational components to properly manage and monitor its boundaries. The Maritime Security Capstone IPT is responsible for gathering and prioritizing the requirements from a variety of members and stakeholders, including: U.S. Coast Guard (USCG), U.S. Customs and Border Protection (CBP), U.S. Immigrations and Customs Enforcement (ICE), and Transportation Security Administration (TSA). The IPT is focused on improving communication, sensors, and surveillance capabilities for its customer components, leading to better operational situation awareness and management of mission-related information. Deliverables resulting from the deliberations of the Maritime Security IPT will feed and enable DHS policy, cross-component acquisition and procurement decisions through technology development and/or knowledge building.

REPRESENTATIVE TECHNOLOGY NEEDS

- Wide-area surveillance from the coast to beyond the horizon, including port and inland waterways, for detection, ID, & tracking— In particular, the detection of vessels between the port region and beyond the horizon, especially small vessels with the capability to geo-reference the images (Borders and Maritime Security Division)
- Improve the capability to continuously track contraband on ships or containers—in particular the ability to conceal transponders while maintaining effective transmissions (Borders and Maritime Security Division)
- Vessel compliance through less-lethal compliance methods—in particular, exploring a variety of technical approaches to interdict illegal migrant operations, contraband transport, fishing, security threats, or general law violations (Borders and Maritime Security Division)
- Ability for law enforcement personnel to detect and identify narcotics, chemical warfare agents, toxic industrial chemicals, explosives, and contraband materials—in particular, a safe, lightweight, non-intrusive inspection device for chemicals, explosives, and drugs featuring one-step operation and able to identify multiple threats (chemical warfare agents, toxic industrial chemicals, explosive chemicals, drugs) with one unit/one setup, operating on portable power, wearable, self-contained, using non-contact methodology to sample suspected contraband items (Borders and Maritime Security Division)
- Improved radar performance for detection and tracking of large and small vessels in the port and coastal regions—in particular, through the use of more advanced signal processing (Borders and Maritime Security Division)

Anh Duong, Division Head, Borders and Maritime Security
Email: SandT-BordersMaritime@dhs.gov



CYBER SECURITY

DHS Lead: National Cyber Security Center, United States Secret Service, National Protection and Programs Directorate

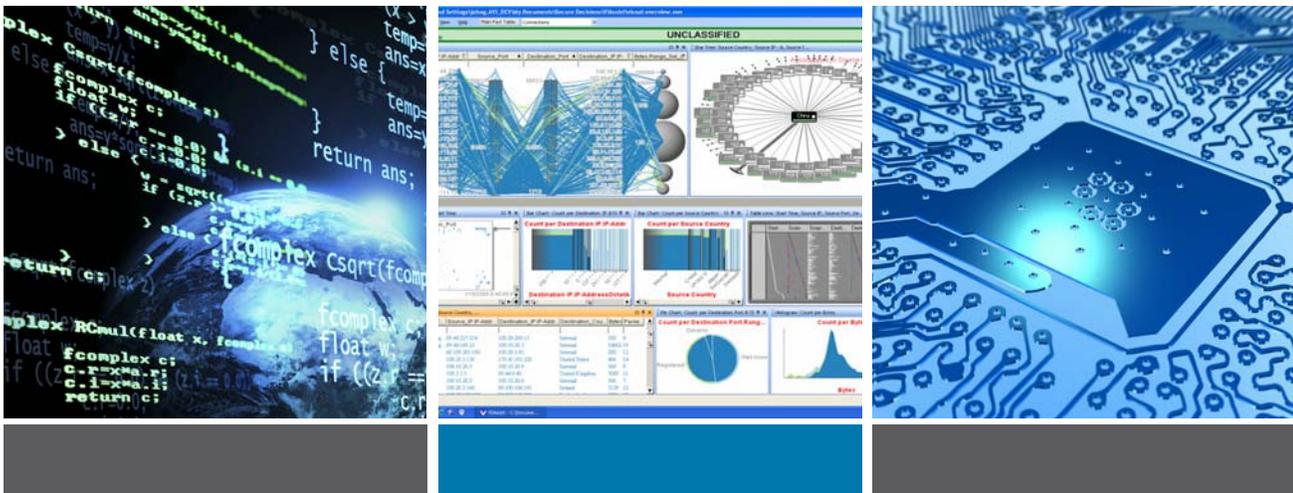
The Cyber Security Capstone IPT provides homeland security practitioners with a toolkit of technologies, processes, and mechanisms to support gathering, analyzing, managing, sharing, and protecting information. The program conducts research, development, testing, evaluation, and transition activities focused on protecting critical information infrastructure; developing the cyber research infrastructure; and delivering new technologies to relevant end users.

REPRESENTATIVE TECHNOLOGY NEEDS

- Secure Internet protocols, including standard security methods (Command, Control and Interoperability Division)
- Improved capability to model the effects of cyber attacks—in particular, measuring security and risk in IT infrastructure components and understanding of Internet topography (Command, Control and Interoperability Division)
- Software Testing and Vulnerability Analysis Technologies—in particular, services and capabilities to rigorously and routinely build, test, and analyze source and binary forms of software in realistic conditions representative of operational environments (Command, Control and Interoperability Division)
- Usable Security—in particular, focused technologies that demonstrate new ways to address the confluence of usability and security (Command, Control and Interoperability Division)
- Information-system insider-threat detection models and mitigation technologies—in particular, technology aids that increase the accuracy, reduce the time, and reduce the cost of detecting and discovering unauthorized insiders (Command, Control and Interoperability Division)
- Analytical techniques for security across the IT system-engineering lifecycle—in particular, analytical techniques to facilitate detecting, quantifying, measuring, visualizing, and understanding system security (Command, Control and Interoperability Division)
- Process Control Systems (PCS) security—in particular capabilities for metrics, wireless communications, and system vulnerability assessment. (Command, Control and Interoperability Division)
- Cyber Forensics—in particular, cyber-related tools and investigative techniques that support law enforcement to address the full range of investigating and solving cyber related crimes (Command, Control and Interoperability Division)

Dave Boyd, Division Head, Command, Control, and Interoperability

Email: SandT-C2I@dhs.gov





INFORMATION SHARING

DHS Lead: Office of Intelligence & Analysis

The Information Sharing Capstone IPT provides homeland security practitioners with a toolkit of technologies, processes, and mechanisms to support gathering, analyzing, managing, sharing, and protecting information. The current information-sharing environment consists of communities that have developed their own policies, rules, standards, architectures, and systems to channel information to meet mission requirements. The Information Sharing program is developing national solutions for sharing all-hazards information in a manner consistent with national security and legal standards that create new technologies to share, search, and analyze homeland security information across jurisdictional boundaries; provide technologies to enable a distributed, secure, and trusted environment for transforming data into actionable information; and recognize and leverage the vital roles played by state and major urban area information fusion centers.

REPRESENTATIVE TECHNOLOGY NEEDS

- Data fusion from law enforcement, intelligence partners, and other sensors to support a user-defined operating picture (UDOP)—in particular, technologies to correlate and fuse sensor data into a comprehensive representation (Command, Control and Interoperability Division)
- Management of user identities, rights, and authorities—In particular, technologies and standards to enable external identity adjudication (Command, Control and Interoperability Division—shared between Information Sharing and Cyber Security)
- Distribution of intelligence products—in particular, technologies and techniques to automate the distribution of unclassified or lower classification portions of intelligence information to DHS mission partners (Command, Control and Interoperability Division)
- Information sharing within and across sectors on terrorist threats—in particular, analytic capabilities for structured, unstructured, and streaming data (Command, Control and Interoperability Division)
- Improvement of situational awareness and decision support horizontally across Federal Law Enforcement and Intelligence partners as well as vertically through Federal, state, local and tribal partners —*in particular, technologies that provide automated, dynamic, real-time data processing and visualization capability and the information sharing protocols that enable them* (Command, Control and Interoperability Division)
- Predictive analytics—in particular, the ability to correlate data and information for recognizing and potentially predicting terrorist attack patterns (Command, Control and Interoperability Division)
- Protection of U.S. citizen personal data—in particular, advanced data integrity techniques to automatically purge or anonymize personally identifiable information (Command, Control and Interoperability Division)
- Improved cross-agency reporting of suspicious activity—in particular, technologies that would improve real-time awareness through alerting others to and sharing information about suspicious activities and persons (Command, Control and Interoperability Division)

Dave Boyd, Division Head, Command, Control, and Interoperability
Email: SandT-C2I@dhs.gov



INFORMATION SHARING

INTEROPERABILITY

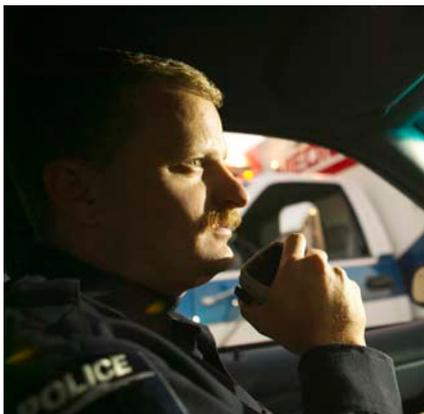
DHS Leads: Federal Emergency Management Agency and Office of Emergency Communications

Relevant and timely information is vital for making tactical, strategic, and planning decisions when responding to natural and man-made incidents and disasters. The Interoperability Capstone IPT provides homeland security practitioners with a toolkit of technologies, processes, and mechanisms to support gathering, analyzing, managing, sharing, and protecting information. The Interoperability program primarily supports the “sharing” aspect by developing solutions related to land mobile radio communications; interoperable voice and data applications; public-safety-grade communications networks; and public alert and warning systems.

REPRESENTATIVE TECHNOLOGY NEEDS

- Accelerate the development of voluntary consensus standards for interoperable communications, including Project 25 and Voice over Internet Protocol. (Command, Control and Interoperability Division)
- Standardize, pilot, and evaluate wireless broadband technologies and applications across multiple networks. (Command, Control and Interoperability Division)
- Develop message interface standards and architectures that enable emergency-information sharing, data exchange, and public alerts and notifications. (Command, Control and Interoperability Division)
- Perform interoperable communications standards compliance testing on emergency response devices and systems. (Command, Control and Interoperability Division)
- Test and evaluate multi-band radio technologies for use in emergency communications and day-to-day operations. (Command, Control and Interoperability Division)
- Develop standards, applications, and technologies to enable seamless access to voice, data, and imagery via a single, unified communications device. (Command, Control and Interoperability Division)
- Develop ad-hoc and mesh networks to link local, state, and Federal personnel in emergency situations and other security events. (Command, Control and Interoperability Division)

Dave Boyd, Division Head, Command, Control, & Interoperability
Email: SandT-C2I@dhs.gov





TRANSPORTATION SECURITY

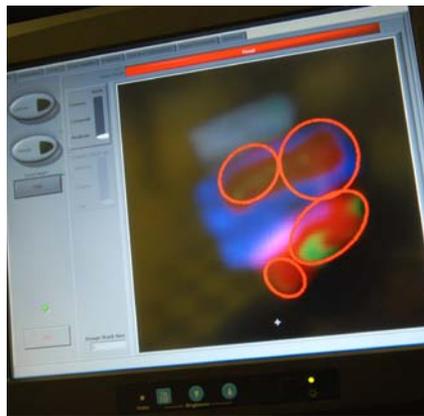
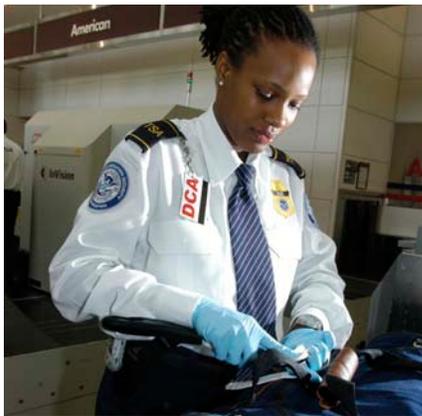
DHS Lead: Transportation Security Administration

Hundreds of thousands of people and tons of cargo move across the nation every day by air, rail, highway, and mass transit systems. The Transportation Security Capstone IPT is pursuing technology solutions that make all modes of transportation safe while still enabling the freedom of movement for people and commerce. Because there is no one technology solution, the IPT takes a layered systems approach to create a strong, formidable system that protects against current and emerging threats.

REPRESENTATIVE TECHNOLOGY NEEDS

- The capability to screen people for explosives and weapons at fixed checkpoints—in particular, technologies that allow higher detection rates with minimal disruption to passenger flow (Explosives Division)
- The capability to detect homemade explosives (HME)—*in particular, characterization of HME threats and damage effects and development of HME detection technologies* (Explosives Division)
- Automated systems solution for explosives and weapons detection in checked and carried baggage—in particular, *automated systems to screen for conventional and homemade explosives and weapons* (Explosives Division)
- Optimization of canine explosive detection capability—in particular, *non-hazardous, low-cost canine training aids* (Explosives Division)
- The capability to screen air cargo for explosives and explosive devices—in particular, technologies for screening break-bulk and palletized air cargo (Explosives Division)

Jim Tuttle, Division Head, Explosives
Email: SandT-Explosives@dhs.gov



COUNTER-IED

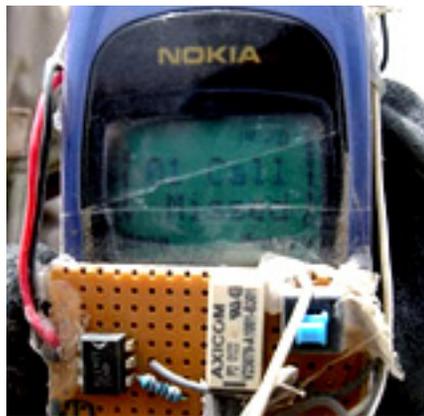
DHS Leads: Office of Bombing Prevention and United States Secret Service

There is no single technology solution to counter the threat of an attack by an improvised explosive device (IED). For this reason, the C-IED Capstone IPT has taken a layered systems approach and is developing technology solutions that can be injected at each stage in the IED attack timeline. (Other emerging counter-IED technology solutions are also being developed in S&T's basic research portfolio).

REPRESENTATIVE TECHNOLOGY NEEDS

- *Capability to identify and model the human precursors of IED threats and terrorist activity within CONUS using unstructured data and novel computational models* (Human Factors/Behavioral Sciences Division)
- *Capability to predict participants and locations of potential IED attacks* based on existing or known geospatial, socio-cultural, and behavioral information (Human Factors/Behavioral Sciences Division)
- *Capability to non-intrusively detect vehicle-borne IEDs—in particular, technologies to detect the explosive or explosive device* (Explosives Division)
- *Capability to detect person-borne IEDs from a standoff distance—in particular, technologies to detect the explosive or explosive device* (Explosives Division)
- *Capability to defeat vehicle-borne IEDs—in particular, non-explosive and standoff defeat technologies* (Explosives Division)
- *Capability to defeat person-borne and leave-behind IEDs* (Explosives Division)
- *Capability to diagnose vehicle-borne and person-borne IEDs* (Explosives Division)
- *Capability to diagnose and defeat water-borne IEDs, above and below the waterline* (Explosives Division)
- *Capability to characterize IED threats, including IED design, assembly, detonation, and effects* (Explosives Division)

Jim Tuttle, Division Head, Explosives
Email: SandT-Explosives@dhs.gov





CHEMICAL/BIOLOGICAL DEFENSE

DHS Leads: Office of Infrastructure Protection and Office of Health Affairs

The Chemical/Biological Defense Capstone IPT improves the understanding, technologies, and systems needed to anticipate, deter, protect against, detect, mitigate, and recover from biological and chemical attacks on the Nation’s population, agriculture, and infrastructure. The program’s mission is “to work to increase the Nation’s preparedness against chemical and biological threats through improved threat awareness, advanced surveillance and detection, and protective countermeasures.”

REPRESENTATIVE TECHNOLOGY NEEDS

- Improved chemical-biological forensic analysis capability (Chemical/Biological Division)
- Handheld rapid biological and chemical detection systems—in particular, technology that distinguishes between threat and non-threat agents and technology to assist with detection and deterrence while the normal stream of commerce continues (Chemical/Biological Division)
- Detection paradigms and systems for improved, emerging, and novel biological threats (Chemical/Biological Division)
- Tools to detect and mitigate animal disease outbreaks (Chemical/Biological Division)
- Analytic tools for accessing and integrating diverse data from multiple domains to enhance biological surveillance (Chemical/Biological Division)
- National-scale detection architectures and strategies to address outdoor and indoor environments (for example, highly trafficked transportation hubs) and critical infrastructure (Chemical/Biological Division)
- Tools to enable assessment of potential consequences of attacks on chemical facilities and chemical–biological attacks on other critical infrastructure (Chemical/Biological Division)
- Integrated CBRNE sensor reporting capability—in particular, the integration of sensors into a common operating picture for easy integration of future detection systems (Chemical/Biological Division)
- New techniques for analysis of chemical threat agent samples, chemical warfare agents, toxic industrial materials and nontraditional agents to develop chemical signatures that supplement traditional forensic techniques. (Chemical/Biological Division)
- Improved tools for integrated CBRN risk assessment (Chemical/Biological Division)
- Incident characterization capability for response and restoration—in particular, fully integrated operational tools to support surveillance, detection, incident characterization, and response systems; plus, a systems approach to characterize the extent of contamination and the restoration of wide urban areas, including high-traffic areas (transit/transportation facilities) following a chemical or biological agent release (Chemical/Biological Division)
- *Integrated system for chemical and biological agent detection in buildings* (Chemical/Biological Division)
- Mechanisms to independently evaluate and validate commercially developed assays for the first-responder community (Chemical/Biological Division)
- *Improved methods of decontamination of biological and chemical contamination from both fixed (e.g., buildings) and moving (e.g., vehicles) infrastructure* (Chemical/Biological Division)
- *Rapid means of interrogation and inspection of closed packages and cargo for illicit chemical and biological threat materials* (Chemical/Biological Division)



Beth George, Division Head, Chemical/Biological
Email: SandT-ChemBio@dhs.gov

PEOPLE SCREENING

DHS Leads: Screening Coordination Office and Citizenship & Immigration Services

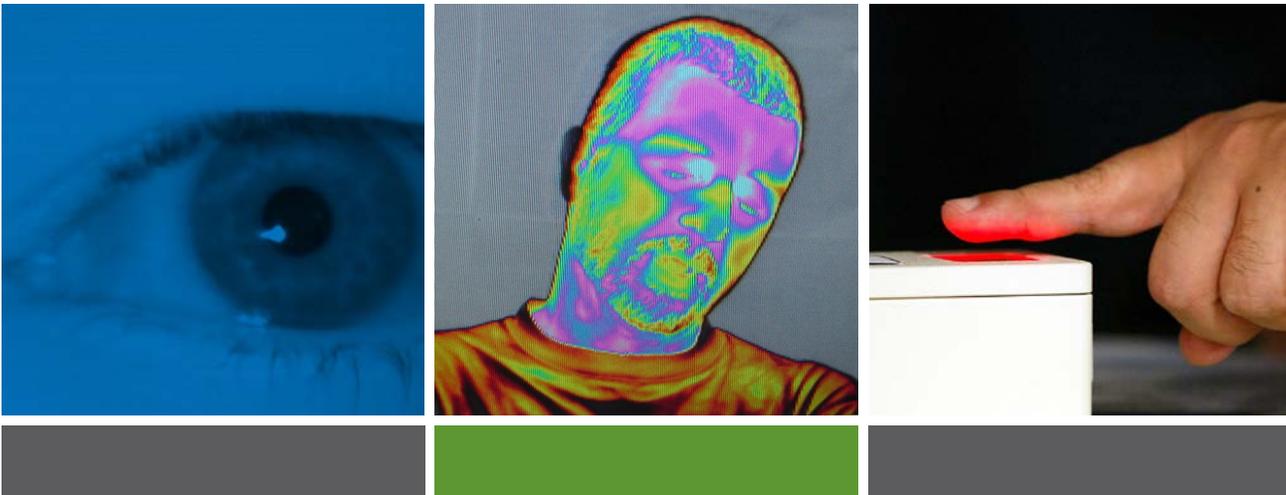
The people Screening Capstone IPT advances national security by developing and applying the social, behavioral, and physical sciences to provide rapid, accurate, non-invasive, user-friendly and publicly acceptable capabilities to improve identification and analysis of unknown and known threats posed by individuals, groups, and radical movements.

REPRESENTATIVE TECHNOLOGY NEEDS

- Systematic collection and analysis of information related to understanding a terrorist group's intent to engage in violence—in particular, data fusion and modeling and simulation capability to provide a near-real-time assessment (Human Factors/Behavioral Sciences Division)
- Real-time detection of deception or hostile intent—in particular, the development of non-invasive behavioral sensors *and analytical methods* (Human Factors/Behavioral Sciences Division)
- Capability to acquire biometrics in challenging operational environments and provide real-time positive verification of an individual's identity, using multiple biometrics—in particular, face, fingerprint, and iris biometrics (Human Factors/Behavioral Sciences Division)
- Mobile biometrics screening capabilities, including handheld, ten-fingerprint-capture, face and iris, environmentally hardened, wireless, and secure devices (Human Factors/Behavioral Sciences Division)
- High-speed, high-fidelity, ten-print capture capability (Human Factors/Behavioral Sciences Division)
- Rapid, cost-effective DNA testing to verify family relationships during interviews for the disposition of benefits (*under \$100 per test; ultimately within 45 minutes for testing*) (Human Factors/Behavioral Sciences Division)
- Remote, standoff biometric detection for identifying individuals at a distance (Human Factors/Behavioral Sciences Division)
- Maximize screener performance at checkpoints through selection and training, and through the use of advanced imaging technologies. (Human Factors/Behavioral Sciences Division)

Sharla Rausch, Division Head, Human Factors/Behavioral Sciences

Email: SandT-HumanFactors@dhs.gov



INFRASTRUCTURE PROTECTION

DHS Lead: Office of Infrastructure Protection

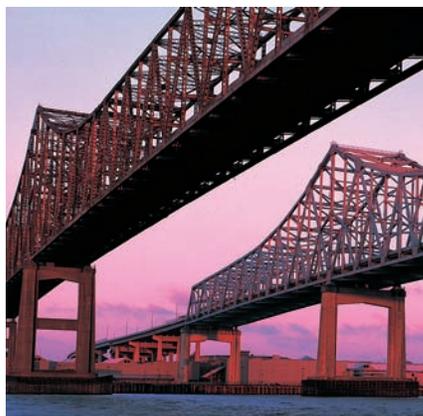
The Infrastructure Protection Capstone IPT mission is to improve the Nation’s preparedness for, and response to, natural and man-made threats to critical infrastructure. The IPT develops technical solutions and reach-back capabilities to improve Federal, state, local, tribal, and private-sector preparedness and response efforts to all-hazards events that impact the Nation’s critical infrastructure. The primary Federal customers for the IPT are the Department of Homeland Security’s (DHS’s) Office of Infrastructure Protection (IP), the National Protection and Programs Directorate (NPPD), and critical infrastructure owners and operators.

REPRESENTATIVE TECHNOLOGY NEEDS

- High-Resolution Analytical tools to accurately quantify interdependencies and cascading consequences as disruptions occur across critical infrastructure sectors—in particular, *tools for natural and man-made disruptions* (Infrastructure and Geophysical Division)
- Effective and affordable blast analysis and protection for critical infrastructure; improved understanding of blast failure mechanisms and protection measures for the most vital assets through the development of suites of advanced materials, design procedures, and innovative construction methods to protect CI/KR (Infrastructure and Geophysical Division)
- Advanced, automated and affordable monitoring and surveillance—in particular, decision support systems, and mitigation strategies to prevent disruption and build in resiliency (Infrastructure and Geophysical Division)
- Rapid mitigation and recovery technologies to quickly reduce the effect of natural and man-made disruptions and cascading effects (Infrastructure and Geophysical Division)
- Critical utility components that are affordable, highly transportable, and provide robust solutions during man-made and natural disruptions (Infrastructure and Geophysical Division)
- *Systems to provide early warning capabilities for early detection and notice of potential levee failures* (Infrastructure and Geophysical Division)

Chris Doyle, Division Head, Infrastructure and Geophysical

Email: SandT-InfrastructureGeophysical@dhs.gov



INCIDENT MANAGEMENT

DHS Leads: Federal Emergency Management Agency and Office of Emergency Communications

The Incident Management Capstone IPT mission is to improve the Nation's preparedness for, and response to, natural and man-made threats through superior situational awareness and emergency response capabilities. The IPT develops technical solutions and reach-back capabilities to improve Federal, state, local, tribal, and private-sector preparedness and response efforts to all-hazards events that impact the United States' people and economy. The primary Federal customer for the IPT is the Federal Emergency Management Agency (FEMA), which represents end users, including first responders and Federal, state, and local emergency managers.

REPRESENTATIVE TECHNOLOGY NEEDS

- Integrated modeling, mapping, and simulation capability—in particular, an integrated and simulation-based incident planning and response capability to analyze all-hazard disaster response and recovery operations, tactics, techniques, plans, and procedures for use in a real-time environment for simulation-based training (Infrastructure and Geophysical Division)
- Personnel monitoring (emergency responder 3-D locator system) capability—in particular, *X/Y/Z accuracy of better than 1 meter in a multilevel building providing incident commanders the ability to rapidly track and effectively deploy or redeploy first responders in a challenging environment* (Infrastructure and Geophysical Division)
- Personnel monitoring (physiological monitoring of firefighters) capability—in particular, *an integrated body-worn sensor suite to provide real-time health analysis and issue alarms to both wearer and command staff, reducing risk of responder cardio/cerebral fatalities through early identification and mitigation* (Infrastructure and Geophysical Division)
- Incident management enterprise system—in particular, increased situational awareness to manage available and anticipated human and material resources, transportation capabilities, and the need for timely information to support critical decisions involving rapidly shifting priorities; geospatial data to create a seamless system between Federal, state, and local first responders; and established virtual continuity of operations (COOP) capabilities to improve incident management when key infrastructures and facilities are unavailable (Infrastructure and Geophysical Division)
- Logistics management tool—in particular, *technologies to effectively manage critical resources and provide complete resource situational awareness at all levels of government, down to point of consumption, and return* (Infrastructure and Geophysical Division)

Chris Doyle, Division Head, Infrastructure and Geophysical

Email: SandT-InfrastructureGeophysical@dhs.gov



Doing Business with DHS S&T:

All U.S. Government business opportunities can be found at www.fedbizopps.gov.

- **HSARPA:** Register to join the HSARPA mailing list to receive various meeting and solicitation announcements. Link to the Long Range Broad Agency Announcement solicitation, where multiple awards are anticipated and will be based upon the proposal evaluation, funds availability, and other programmatic considerations. Also link to Representative High Priority Technology Areas, where DHS areas of interest can be found. <http://www.hsarpabaa.com>
- **Small Business Innovation Research (SBIR):** SBIR's goal is to increase the participation of innovative and creative small businesses in Federal Research/Research and Development (R/R&D) programs and challenge industry to bring innovative homeland security solutions to reality. <http://www.sbir.dhs.gov>
- **SAFETY Act:** The SAFETY Act enables the development and deployment of qualified anti-terrorism technologies and provides important legal liability protections for manufacturers and sellers of effective technologies. <https://www.safetyact.gov/>
- **TechSolutions:** The mission of TechSolutions is to rapidly address technology gaps identified by Federal, state, local, and tribal first responders by fielding prototypical solutions within 12 months at a cost less than \$1 million per project. www.dhs.gov/techsolutions
- **The Long Range BAA** identifies strategic topics of interest to DHS's mission and is the a principal vehicle for white papers and full proposals. Submissions are assessed based on the stated evaluation criteria and the overall best value to the government. <https://baa.st.dhs.gov/>



Commercialization Office

The U.S. Department of Homeland Security (DHS), Science and Technology (S&T) Directorate's commercialization efforts are headed by the Commercialization Office, which was officially established in October 2008. The mission of the Commercialization Office is to develop and execute programs and processes that identify, evaluate, and commercialize widely distributed products or services that meet the detailed operational requirements of DHS's operating components, the first responder community, critical infrastructure/key resources (CI/KR) owners and operators, and other Department users. Managing and enhancing DHS S&T's outreach effort with the private sector to establish and foster mutually beneficial working relationships leading to the fielding of technologies to secure the Nation is a primary day-to-day function of the Commercialization Office.

The SECURE Program—one of the Commercialization Office's innovative public-private partnerships enables the rapid, cost-effective and efficient development of products and services to protect the Homeland to the benefit of the taxpayers, the private sector, and DHS. The goal of the SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) program is to leverage the resources of the private sector to develop solutions aligned with (and tested against) DHS-generated and vetted detailed operational requirements, using the private sector's experience and resources. DHS stakeholders can then make better-informed decisions on products or services specifically aligned to their requirements. (See http://www.dhs.gov/xres/programs/gc_1211996620526.shtm)

COMMERCIALIZATION OFFICE RESOURCES

In order to facilitate outreach to the private sector and improve communications, the Commercialization Office has published a number of materials, including briefs, books, and articles that outline the major activities of the Commercialization Office and provide readers with easy-to-understand guides for requirements developed and the recently developed and implemented DHS commercialization process. The Commercialization Office also reaches out to businesses of all kinds—disadvantaged, small, medium and large—about opportunities that exist for partnership. The Commercialization Office makes these resources available to all who are interested. Please visit our Web site at http://www.dhs.gov/xabout/structure/gc_1234194479267.shtm.

Requirements Development Resources: The Commercialization Office has published three popular books to assist in the development of detailed operational requirements [*Requirements Development Guide* (April 2008), *Developing Operational Requirements* (May 2008), and *Developing Operational Requirements, Version 2* (November 2008)]. These books serve as useful resources to explain the critical role of detailed requirements in the cost-effective and efficient development of products and services.

Commercialization Office Articles: The Commercialization Office has published more than 25 articles and a compilation of works [“Harnessing the Valuable Experiences and Resources of the Private Sector for the Public Good” (February 2009)] written at the request of the private sector to inform the public of new opportunities and ways to work with DHS. The articles inform readers about processes and the benefits of fostering a mutually beneficial partnership with DHS. Article topics include the critical role of requirements, focus the role of small and disadvantaged businesses, global outreach efforts and potential available markets.

Other Resources: In addition, the Commercialization Office has made available a number of presentations, a program concepts-of-operations, and a product realization chart that correlates terminology used by both the public and private sector to delineate how science, technology development, and product development are related to basic research, innovation, and transition, using a Technology Readiness Level (TRL) “backbone.”

Feedback Welcomed! For more information on how to get involved in programs like SECURE or to provide feedback to the Commercialization Office, please send an e-mail to sandt_commercialization@hq.dhs.gov.

Frequently Asked Questions

1. Who submits a technology need for consideration?

DHS solicits requirements inputs from all communities that carry out Homeland Security missions, such as DHS Components (Coast Guard, ICE, CBP, ICE, TSA, Secret Service, and FEMA etc), end users, first responders, and state, local, and tribal authorities.

2. What is the benefit from working with DHS S&T?

Working with DHS S&T can provide business opportunities to:

- Provide technical services and expertise that address important National Security needs.
- Develop and manufacture widely distributed products for end users.
- Better understand DHS current and future needs to effectively respond to DHS solicitations.

3. Is DHS S&T interested in assessing existing products that appear to meet or address a technology need identified here?

YES. If you believe you have a product that meets or addresses a need stated in this booklet, email the division point of contact (POC) for the Capstone IPT relevant to your field. State which need your product addresses and briefly provide any supporting material that describes your product and how it specifically addresses that need. Your email will be directed to a Subject Matter Expert (SME) within the division for evaluation and assessment. You will be notified of the division's interest in pursuing further discussions with you regarding your product.

4. What is the best way to determine DHS S&T interest in a research idea?

First contact the S&T POC whose division best matches the research field of interest. This person will attempt to match up the research or technology development with the correct person(s) within the S&T Directorate. Those contemplating submission of a white paper or full proposal may obtain valuable insight about whether their expertise and interest is a good match for research currently being funded by S&T.

If interest is indicated, The Long Range BAA is a principal vehicle for submitting white papers and full proposals. It is recommended that a white paper be the first step before expending the time and expense of submitting a full proposal. Submissions are assessed based on the stated evaluation criteria and overall best value to the government. Multiple contract awards can be made based upon the proposal's evaluation, funding availability and priorities, and other programmatic considerations. Awards may take the form of contracts, grants, cooperative agreements, or other transaction (OTAs) agreements, as appropriate.

DHS S&T Points of Contact:

- ▶ **Starnes Walker**
Director of Research
Email: SandT-Research@dhs.gov
- ▶ **Roger McGinnis**
Director of Innovation
Email: SandT-Innovation@dhs.gov
- ▶ **Rich Kikla**
Director of Transition
Email: SandT-Transition@dhs.gov
- ▶ **Randel Zeller**
Director of Interagency and First Responder Programs
Email: IAD-FirstResponder@dhs.gov
- ▶ **Jim Tuttle**
Division Head, Explosives
Email: SandT-Explosives@dhs.gov
- ▶ **Beth George**
Division Head, Chemical/Biological
Email: SandT-ChemBio@dhs.gov
- ▶ **Dave Boyd**
Division Head, Command, Control, and Interoperability
Email: SandT-C2I@dhs.gov
- ▶ **Anh Duong**
Division Head, Borders and Maritime Security
Email: SandT-BordersMaritime@dhs.gov
- ▶ **Sharla Rausch**
Division Head, Human Factors/Behavioral Sciences
Email: SandT-HumanFactors@dhs.gov
- ▶ **Chris Doyle**
Division Head, Infrastructure and Geophysical
Email: SandT-InfrastructureGeophysical@dhs.gov

*From Science and Technology...
Security and Trust*



Appendix N: Market Potential Templates

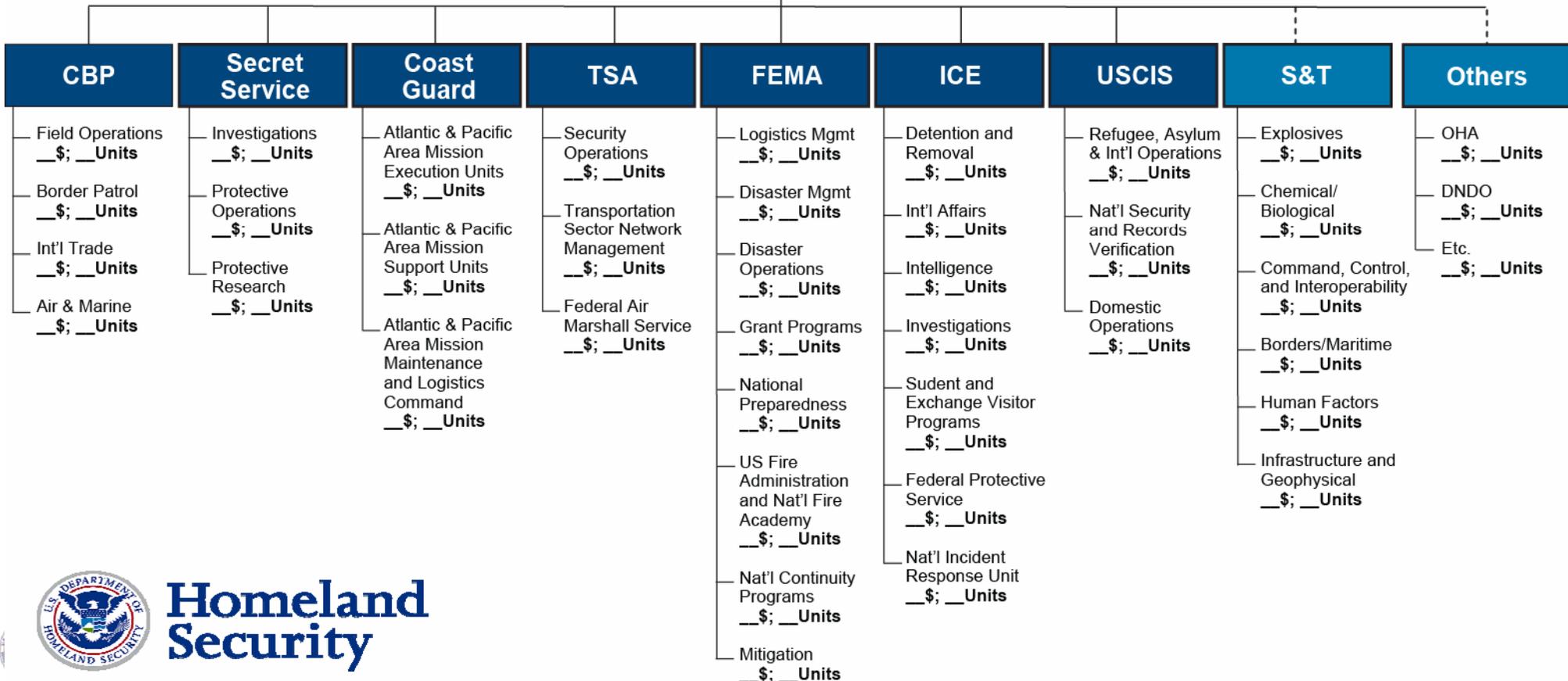
Market Potential Template



DHS

Ancillary Markets

First Responders

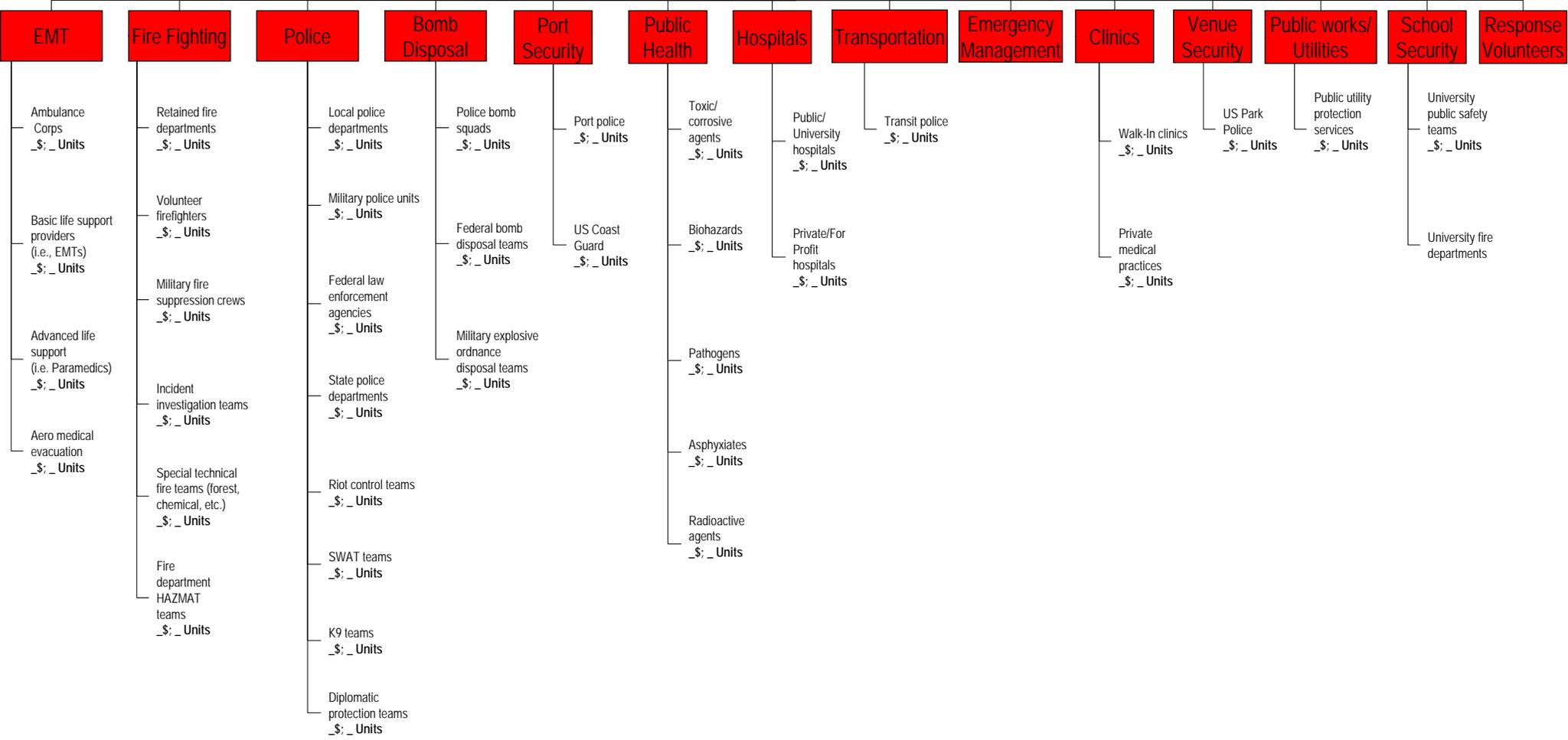


Homeland Security

Critical Infrastructure Key Resources (CIKR)

Agriculture and Food	Defense Industrial Base	Energy	Public Health and Healthcare	National Monuments and Icons	Banking and Finance	Water	Chemical	Commercial facilities	Emergency Services	Materials, Reactors and	Telecommunications	Critical Manufacturing	Postal and Shipping Services	Transportation	Information Technology
Food Retail _\$_; _ Units	Defense Contractors _\$_; _ Units	Coal mining operations _\$_; _ Units	Public/University hospitals _\$_; _ Units	Guided tour services _\$_; _ Units	Credit lending institutions _\$_; _ Units	Public utilities _\$_; _ Units	Inorganic chemical production _\$_; _ Units	Hotels _\$_; _ Units	Fire Departments _\$_; _ Units	Electric utilities _\$_; _ Units	Telephone/Cellular services _\$_; _ Units	Iron and Steel mills _\$_; _ Units	United States Postal Service _\$_; _ Units	AMTRAK _\$_; _ Units	Hardware providers _\$_; _ Units
Farm Equipment _\$_; _ Units	Industry analysis _\$_; _ Units	Coal power plants _\$_; _ Units	Private/For Profit hospitals _\$_; _ Units	Travel services _\$_; _ Units	Commercial banking _\$_; _ Units	Desalinization plants _\$_; _ Units	Organic industrial production _\$_; _ Units	Shopping centers _\$_; _ Units	Law enforcement agencies _\$_; _ Units	Reactor and associated materials _\$_; _ Units	Satellite data transmission _\$_; _ Units	Aluminum production and processing _\$_; _ Units	High volume document and parcel shipping _\$_; _ Units	Commuter rail _\$_; _ Units	IT Conglomerates _\$_; _ Units
Meat/Poultry Processing _\$_; _ Units	Think tanks/research institutions _\$_; _ Units	Coal equipment manufacturers _\$_; _ Units	Clinics _\$_; _ Units	Lodging/Hotel _\$_; _ Units	Private equity _\$_; _ Units	Treatment plants _\$_; _ Units	Ceramics _\$_; _ Units	Stadiums and sport arenas _\$_; _ Units	Search and rescue teams _\$_; _ Units	University and educational institutions _\$_; _ Units	Broadcasting entities _\$_; _ Units	Nonferrous metal production and processing _\$_; _ Units	Container shipping services _\$_; _ Units	Intracity rail services _\$_; _ Units	Semiconductor production _\$_; _ Units
Food Processing _\$_; _ Units	University partnership programs _\$_; _ Units	Hydroelectric _\$_; _ Units	Private medical practices _\$_; _ Units	Guest services/tourist hospitality _\$_; _ Units	Consumer banking _\$_; _ Units	Equipment manufacturers _\$_; _ Units	Petrochemicals _\$_; _ Units	Schools _\$_; _ Units	Ambulance companies _\$_; _ Units	Control systems _\$_; _ Units	Broadcast equipment manufacturing _\$_; _ Units	Engine, Turbine and Power transmission _\$_; _ Units	Marine shipping _\$_; _ Units	Commercial airline _\$_; _ Units	Electronics manufacture _\$_; _ Units
Dairy Processing _\$_; _ Units	National laboratories _\$_; _ Units	Dam operations _\$_; _ Units	Medical laboratories _\$_; _ Units	People moving services _\$_; _ Units	Building societies/Private banks _\$_; _ Units	Pipe and water control device manufacturers _\$_; _ Units	Agrochemicals _\$_; _ Units	Commercial office buildings _\$_; _ Units	Mountain/Cave/ Mine rescue teams _\$_; _ Units	Nuclear safety systems _\$_; _ Units	Radio equipment manufacturing _\$_; _ Units	Marine shipping _\$_; _ Units	Trucking industry _\$_; _ Units	Private air services _\$_; _ Units	IT services _\$_; _ Units
Dairy Farms _\$_; _ Units		Wind power _\$_; _ Units	Pharmaceutical _\$_; _ Units	Queuing equipment makers _\$_; _ Units	Merchant banks _\$_; _ Units		Polymers _\$_; _ Units	Museums _\$_; _ Units	Other technical rescue teams _\$_; _ Units	Waste disposal services _\$_; _ Units	Electrical equipment manufacturing _\$_; _ Units	Airborne shipping _\$_; _ Units	Cruise lines _\$_; _ Units	Server and network hardware _\$_; _ Units	IT services _\$_; _ Units
Ranching _\$_; _ Units		Solar power _\$_; _ Units	Health insurance _\$_; _ Units	Private security _\$_; _ Units	Global financial services firms _\$_; _ Units		Elastomer production _\$_; _ Units	Zoos and Aquariums _\$_; _ Units	Bomb disposal units _\$_; _ Units	Uranium processors _\$_; _ Units	Motor Vehicle manufacturing _\$_; _ Units	Trucking industry _\$_; _ Units	Subway systems _\$_; _ Units	Server and network hardware _\$_; _ Units	IT services _\$_; _ Units
Organic Farming/Sustainable Agriculture _\$_; _ Units		Public utilities companies _\$_; _ Units	Medical material providers _\$_; _ Units		Community development _\$_; _ Units		Oleochemicals _\$_; _ Units	Public Libraries _\$_; _ Units	Blood/Organ transplant supply _\$_; _ Units	Protective garment manufacturers _\$_; _ Units	High speed data transmission _\$_; _ Units	Aerospace product & parts manufacturing _\$_; _ Units	Subway systems _\$_; _ Units	Server and network hardware _\$_; _ Units	IT services _\$_; _ Units
Traditional Planting _\$_; _ Units		Oil companies _\$_; _ Units	Medical equipment manufacturers _\$_; _ Units		Community banks _\$_; _ Units		Explosives _\$_; _ Units	Amusement parks _\$_; _ Units	Amateur radio emergency comms _\$_; _ Units	Protective garment manufacturers _\$_; _ Units	Internet service providers _\$_; _ Units	Railroad rolling stock _\$_; _ Units	Long-haul maritime shipping _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
Commercial fishing _\$_; _ Units			Medical technology manufacturers _\$_; _ Units		Savings and Loans _\$_; _ Units		Fragrance production _\$_; _ Units		Public utility protection providers _\$_; _ Units	Print media _\$_; _ Units	Internet technology providers _\$_; _ Units	Other Transportation equipment _\$_; _ Units	Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
			Biotechnology _\$_; _ Units		Credit unions _\$_; _ Units		Chemical wholesale _\$_; _ Units		Emergency Road services _\$_; _ Units	Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
					Insurance companies _\$_; _ Units		Exotic chemicals _\$_; _ Units		Emergency Social services _\$_; _ Units	Print media _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
					Insurance brokerages _\$_; _ Units				Community emergency response teams _\$_; _ Units	Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
					Reinsurance companies _\$_; _ Units				Disaster relief _\$_; _ Units	Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
					Stock brokerages _\$_; _ Units				Famine relief teams _\$_; _ Units	Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
					Capital market banks _\$_; _ Units				Poison Control units _\$_; _ Units	Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
					Custody services _\$_; _ Units				Animal control teams _\$_; _ Units	Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
					Angel investment _\$_; _ Units				Wildlife services _\$_; _ Units	Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
					Venture capital _\$_; _ Units					Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units			Software production _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
										Internet service providers _\$_; _ Units					

First Responders



Appendix O: Product Realization Chart



U.S. Department of Homeland Security: Commercialization Office

Product Realization Chart

DHS S&T Portfolio	N/A			Basic Research			Innovation and Transition				
Technology Phase	Needs Assessment			Science			Technology Development		Product Development		
Technology Readiness Level (TRL)	N/A			TRL 1 – TRL 3			TRL 4 – TRL 6		TRL 7 – TRL 9		
Key Objectives	<ul style="list-style-type: none"> Identify S&T capability gaps (mission needs) requiring material solutions. Preliminary operational requirements are developed. Market survey. Technology scan. Assess technology-based solutions to address gaps. Develop rough order-of-magnitude (ROM) estimates of project cost and schedule. Investigate the value proposition of a product idea. Establish technical objectives and milestones. Conduct preliminary IP review. Ensure the qualification of tools, materials, processes, and suppliers as required. Provide a preliminary production plan. Develop preliminary marketing objectives and milestones. Initiation of Congressional Appropriations Memo, Technology Transition Agreements (TTA), Program Descriptions (Research and Innovation), and Feasibility Studies lead to Program and Budget Execution. List other objectives when defined. 	<ul style="list-style-type: none"> A program sponsor and end-users / requirements have been identified. Mission Needs Statement has been developed. Communication with end-users and customers has been initiated. Preliminary operational requirements have been developed. A Feasibility Study White Paper has been developed and accepted. (TRL1 and 2) A threat, vulnerability, or gap has been identified. Develop and update the preliminary product plan. List other objectives when defined. 	<ul style="list-style-type: none"> End-user is involved in concept and requirements development. An empirical or theoretical design solution has been proven in laboratory experiments. Analytical studies to confirm the basic principles of the technology have been developed. Operational requirements analysis has been conducted; Operational requirements are applied to Functional Requirements. (TRL 2 and 3) System concept(s) / architecture have been assessed. Program Risk Assessment has been developed; Risk Management Plan has been developed. (TRL 2 and 3) Program Cost Analysis has been completed and updated. (TRL 2 and 3) Preliminary Security Assessment has been conducted. Develop a Technology Roadmap. Refine the market assessment and technology scan. List other objectives when defined. 	<ul style="list-style-type: none"> Supplemental and alternate technologies throughout DHS S&T have been surveyed. Technology's physical validity has been proven in laboratory experiments. Program Management Plan (PMP) has been developed. Proof of Concept Plan has been developed. Manufacturing / production strategy has been developed. Develop Quality Control Plan to include standards conformance, reliability testing, etc. Develop Marketing Plan to include market size and research. List other objectives when defined. 	<ul style="list-style-type: none"> All required technology components are integrated for Proof of Concept. Proof of Concept is conducted. IPIT has certified readiness for the technology's development. The customer has been briefed on the Proof of Concept results. Functional Requirements Document has been finalized. SEMP has been finalized and updated. (TRL 4, 5, & 6) TEMP has been completed and updated. (TRL 4, 5, & 6) Configuration Management Plan exists. PMP has been updated. (TRL 4, 5, and 6) Risk Management Plan is updated. (TRL 4, 5, and 6) Program Cost Analysis is updated. (TRL 4, 5, and 6) Quality Assurance Plan exists. Program Transition Manager is engaged in transition planning. List other objectives when defined. 	<ul style="list-style-type: none"> ORD and CONOPS are developed. Security Assessment is updated. OMB 300 and Acquisition Plan have been completed (if required). IPIT has certified readiness for the transition of the Technology. Program Transition Manager has assisted in transition documentation development. Technology scan and market survey. (ongoing) Analysis of Alternatives is developed and updated. (TRL 5 & 6) Entry Criteria Checklist is completed and delivered to the TM. POD has been created, approved, and signed. (TRL 5 & 6) Director has approved the transition. List other objectives when defined. 	<ul style="list-style-type: none"> Germane to both Acquisition and Commercialization Execute a preliminary Technology Transition Agreement (TTA), or Technology Commercialization Agreement (TCA) as applicable Program Manager has been identified Successful T&E in a simulated operational environment has been conducted. End user / customer has been briefed on the results of T&E. Initial Security Guidelines have been developed. Draft Program Assessment Rating Tool (PART) plan exists, if required. National Environmental Policy Act (NEPA) plan / assessment, if required. Interoperability Assessment. List other objectives when defined. 	<ul style="list-style-type: none"> Germane to both Acquisition and Commercialization S&T and the end-user / customer have begun to develop transition planning document; Transition Plan has been developed. (TRL 7 and 8) Technology has been successfully demonstrated in an operational environment. (TRL 7 and 8) Updates (if required) have been made to the Operational and / or Functional Requirements Document. Risk Management Plan, Program Cost Analysis and PMP have been updated (as needed). Strategic Program Planning (e.g., Balanced Scorecard) has been conducted. Operations and Maintenance Manual has been completed / updated. Security Manual has been developed. Interoperability has been demonstrated. Management Directives (MD) have been reviewed to assure compliance. List other objectives when defined. 	<ul style="list-style-type: none"> Germane to both Acquisition and Commercialization Technology components are form, fit, and function compatible with an operational system. Technology production has been addressed and planned by DHS and the end-user / customer. Training Plan has been developed and implemented. (TRL 8 and 9) Operational Test Report has been completed. Limited User Test (LUT) Plan has been developed. List other objectives when defined. 	<ul style="list-style-type: none"> Germane to both Acquisition and Commercialization All critical program documentation has been completed. Planning is underway for the integration of the next generation technology into the existing program components. End-user fully demonstrates the technology in CONOPS. Lessons Learned completed. After Action Review completed. Sustainment Plan is completed. List other objectives when defined. 	
Key Deliverables	<ul style="list-style-type: none"> Preliminary market assessment and technology scan. Congressional Appropriations Memo, Technology Transition Agreements, Program Descriptions (Research and Innovation), and Feasibility Studies lead to Program and Budget Execution. Preliminary product plan that assesses features, benefits, and risk. Initial plan for marketing, production, and sales control. List other deliverables when defined. 	<ul style="list-style-type: none"> Mission Needs Statement. Feasibility Study. Program Management Vision, or Description of Leap-ahead Capability. Written report of findings and recommendations (preliminary product plan). Feasibility Review meeting. List other deliverables when defined. 	<ul style="list-style-type: none"> Preliminary Operational Requirements Document (end-user / customer validation). Program Cost Analysis (updated). (TRL 2 and 3) Program Risk Assessment (technology, schedule, etc.). Risk Management Plan (TRL 2 and 3) Preliminary Security Assessment. Functional Requirements (draft). (TRL 3) Preliminary product plans (approved and ongoing). New Technology roadmaps (approved for further development and implementation). Updated market assessment and technology scan. List other deliverables when defined. 	<ul style="list-style-type: none"> Systems Engineering Management Plan (SEMP) draft. Proof of Concept Plan. Program Management Plan (PMP) draft. End-user / Customer Status Review. Detailed product and marketing plan. Quality control plan. Optimization Review meeting. List other deliverables when defined. 	<ul style="list-style-type: none"> Proof of Concept Report. Functional Requirements Document. SEMP (TRL 4, 5, and 6) TEMP (TRL 4, 5, and 6) Quality Assurance Plan. Configuration Plan Management. PMP (updated). (TRL 4, 5, & 6) Risk Management Plan (updated). (TRL 4, 5, and 6) Program Cost Analysis (updated). (TRL 4, 5, and 6) End-user / Customer Status Review. List other deliverables when defined. 	<ul style="list-style-type: none"> ORD and CONOPS. Security Assessment (updated). Program Definition Document (PDD). OMB 300 Capital Asset Plan. Acquisition Plan. Entry Criteria Checklist. Analysis of Alternatives. (TRL 5 & 6) List other deliverables when defined. 	<ul style="list-style-type: none"> Germane to both Acquisition and Commercialization Technology Transition Agreement (TTA), or Technology Commercialization Agreement (TCA) as applicable Initial Security Guidelines. Draft Program Assessment Rating Tool (PART) plan, if required. National Environmental Policy Act (NEPA) initial assessment, if required. Interoperability Assessment. List other deliverables when defined. 	<ul style="list-style-type: none"> Germane to both Acquisition and Commercialization Transition Plan (draft) Operational and Functional Requirements Documentation (updated). Risk Management Plan (updated). Program Cost Analysis (updated). PMP (updated). Strategic Program Planning (updated) (if conducted). Operations and Maintenance Manual. Security Manual. Finalized Interoperability Assurance Report. (TRL 7 and 8) Applicable Management Directives (MD), if required. (TRL 7) List other deliverables when defined. 	<ul style="list-style-type: none"> Germane to both Acquisition and Commercialization Limited User Test (LUT) Plan. Deployment or Transition Plan. Training Plan. Operational Test Report. Customer Acceptance Document. Initial Systems-level Metrics Assessment. List other deliverables when defined. 	<ul style="list-style-type: none"> Germane to both Acquisition and Commercialization Customer Feedback. Lessons Learned. After-action Review. Sustainment Plan is completed (a. Spiral Development Assessment, b. Predefined Product Improvement, c. Emerging Threats) Assessment, d. Technology Refresh / Insertion, e. Quality Assurance / Metrics Report, f. Risk Management Reassessment). List other deliverables when defined. 	
			FutureTECH Program								
							<ul style="list-style-type: none"> Engineering documentation package (release and manufacturing plan). Updated marketing plan. Test plan for quality control. Development Phase Review meeting. List other deliverables when defined. 	<ul style="list-style-type: none"> IP Protection and Licensing. Manufacturing and sales plan release package is to be distributed. Sales Release Phase Review meeting. Pilot Phase Review meeting. List other deliverables when defined. 	<ul style="list-style-type: none"> Demonstrate that a defect-free product can be manufactured on schedule and at a cost consistent with the target price points. List other deliverables when defined. 	<ul style="list-style-type: none"> Finalized product plan sales release package is to be distributed. Execution of the acceptance, shipment, and after-sales support of the new product. List other deliverables when defined. 	
Management Review	<ul style="list-style-type: none"> Corporate review meeting of value proposition and product overview. Results and follow up actions. 	<ul style="list-style-type: none"> Corporate review meeting of the preliminary product plan. Feasibility Review meeting. Results and follow up actions. 	<ul style="list-style-type: none"> Corporate review meeting to approve preliminary product plan and technology roadmap. Results and follow up actions 	<ul style="list-style-type: none"> Optimization Review meeting. Results and follow up actions. 	<ul style="list-style-type: none"> Analysis of the engineering and manufacturing plan. Results and follow up actions. 	<ul style="list-style-type: none"> Analysis of the engineering and manufacturing plan. Results and follow up actions. 	<ul style="list-style-type: none"> Development Phase Review meeting. Comprehensive analysis of the engineering and manufacturing plan. Results and follow up actions. 	<ul style="list-style-type: none"> Corporate review of the manufacturing release package. Pilot Phase Review meeting. Results and follow up actions. 	<ul style="list-style-type: none"> Analysis and review of the manufacturing plan. Results and follow up actions. 	<ul style="list-style-type: none"> Corporate review of the finalized product plan and sales release package. Sales Release Phase Review meeting. 	

