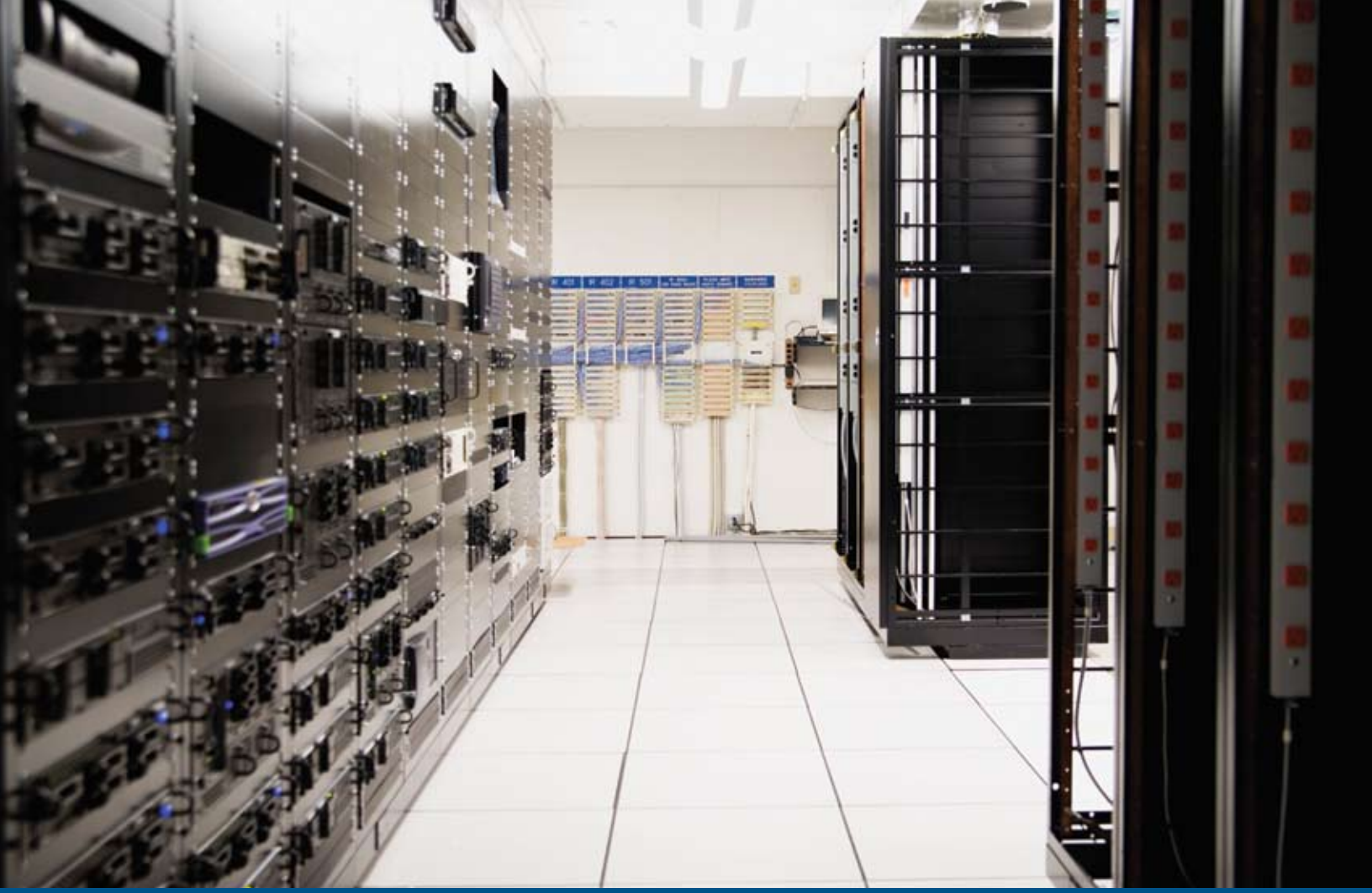


Information Technology

Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan

May 2007

Homeland Security

Information Technology Sector Government Coordinating Council Letter of Concurrence

The National Infrastructure Protection Plan (NIPP) provides the unifying structure for the integration of critical infrastructures and key resources (CI/KR) protection efforts into a single national program. The NIPP provides an overall framework for integrating programs and activities that are underway in the various sectors, as well as new and developing CI/KR protection efforts. The NIPP includes 17 sector-specific plans (SSPs) that detail the application of the overall risk management framework to each specific sector.

Each SSP describes a collaborative effort between the private sector; State, local, and tribal governments; nongovernmental organizations; and the Federal Government. This collaboration will result in the prioritization of protection initiatives and investments within and across sectors to ensure that resources can be applied where they contribute the most to risk mitigation by lowering vulnerabilities, deterring threats, and minimizing the consequences of attacks and other incidents.

Over the past year, the Department of Homeland Security (DHS) worked closely with members of the Information Technology (IT) Government Coordinating Council (GCC), including representatives from the Departments of Commerce, Defense, Justice, State, and Treasury, the Office of the Director of National Intelligence, the Office of Management and Budget, and the National Association of State Chief Information Officers, to develop the IT SSP in partnership with the IT Sector Coordinating Council (SCC). GCC members contributed time and expertise to develop and finalize the IT SSP and will:

- Support the concepts and processes outlined in the IT SSP to carry out their assigned functional responsibilities regarding the protection of CI/KR as described herein;
- Work with DHS, as appropriate and consistent with their own agency-specific authorities, resources, and programs, to implement programs that enhance CI/KR protection;
- Cooperate and coordinate with DHS, in accordance with guidance provided in Homeland Security Presidential Directive 7, as appropriate and consistent with their own agency-specific authorities, resources, and programs, to facilitate CI/KR protection;

- Develop or modify existing interagency and agency-specific CI/KR plans, as appropriate, to incorporate concepts and actions outlined in the IT SSP; and
- Develop and maintain partnerships for CI/KR protection with appropriate State, regional, local, tribal, and international entities; the private sector; and nongovernmental organizations.

DHS looks forward to continuing to work in partnership with IT GCC and IT SCC representatives and other Sector security partners on the implementation of the IT SSP.

Sincerely,

Robert B. Stephan
Assistant Secretary for
Infrastructure Protection
National Protection and Programs Directorate
Department of Homeland Security
Co-Chair, IT GCC

Gregory Garcia
Assistant Secretary for Cyber Security
and Communications
National Protection and Programs Directorate
Department of Homeland Security
Co-Chair, IT GCC

December 29, 2006

The Honorable Robert B. Stephan
Assistant Secretary for Infrastructure Protection
U.S. Department of Homeland Security
Washington, D.C. 20528
Subject: Letter of Coordination, Information Technology Sector Specific Plan

Dear Mr. Assistant Secretary:

The members of the Information Technology (IT) sector, organized through our Sector Coordinating Council, the IT-SCC, share a commitment to improving America's homeland security through our stewardship of critical technology infrastructures. Furthering our public-private partnership with the Department under the framework of the National Infrastructure Protection Plan (NIPP), in 2006, members of the IT-SCC voluntarily organized to work with the government to develop an IT-Sector Specific Plan (SSP). IT-SCC members committed substantial resources, and working together with DHS' National Cyber Security Division (NCSD), we developed a plan document that details improvements that will enhance national capabilities for (1) prevention and protection through risk management, (2) situational awareness, and (3) response, recovery and reconstitution of America's information technology infrastructure. The resulting plan represents the most comprehensive joint planning effort undertaken by IT-Sector public-private security partners.

Having built consensus for the key elements of the plan, the IT-SCC believes that the document's goals and objectives—while ambitious—chart a course for long-term collaboration with the Federal government, including the Department of Homeland Security. The IT-SSP identifies important specific opportunities for collaborative efforts between and among the private sector, State, local and tribal governments, nongovernmental organizations, and the Federal Government. By working together, private and public IT-sector security partners can prioritize protective initiatives and investments within and across sectors. Such collaboration can ensure that limited government resources are applied effectively and efficiently. Over time this will mitigate risks by reducing vulnerabilities, deterring threats, and minimizing the consequences of incidents. Creating a value proposition for both government and private sector participation in this process is critical to fostering increased resilience across shared infrastructures and the supply chains that enable critical IT Sector functions.

Achieving the goals and objectives of the SSP will present some challenges for both public and private security partners. For example, determining, identifying, and obtaining the necessary resources required to perform national level risk assessments of critical IT sectors functions, enhance incident response programs, or develop new programs to support recovery and reconstitution will require working closely with Congress, to prioritize DHS programs (or eliminating unnecessary programs) to meet the agreed upon objectives of the SSP. Similarly, private enterprises will work to develop business cases to make investments of time and resources of their own in support of SSP objectives.

Of particular importance to our sector and this Plan in relation to the companion documents developed by our peer Critical Infrastructure sectors is our approach to the identification of sector facilities in the National Asset Database (NADB). IT-SCC members appreciate DHS' recognition that the unique and virtual nature of critical IT-sector functions do not translate easily into NADB entries. The criticality of sector functions is situational and dependent on their utilization. Accordingly, the sector is generally focused on a threat-scenario-driven risk assessment approach to ascertaining IT Sector Critical Functions and sub-functions, rather than simply cataloging specific or generic assets owned or operated by individual sector members. Any information entered into the NADB should reflect this industry-led, top-down risk assessment approach based on the identified Sector Critical Functions, and be based upon the decision of individual industry owners and operators acting in cooperation with the Department and other agencies. Through the implementation of the IT SSP risk management process, the IT Sector will work with DHS to understand and protect systems, networks, and functions which have unique characteristics or play essential roles in ensuring national and economic security and public health, safety, and confidence.

The members of the IT community, represented by the IT-SCC, will continue to work with DHS, its other government partners (federal, state, local, and tribal) and other security partners to develop and implement the recommendations embodied in this initial iteration of the IT-SSP. It is hoped that this collaboration will result in assessments of risk to IT architectures and functions in a way that will help better prioritize protection initiatives and investments within the sector. The members of the IT-SCC, while sharing the goals expressed in the plan, recognize that by our sector's consensus participation in the NIPP/SSP process, no specific commitment of individual action can be made.

Thank you for your continued support of the IT Sector as we mobilize our constituencies around critical infrastructure protection. We look forward to working in this partnership and to future interaction with the other Sector Coordinating Councils both bilaterally and via the Partnership for Critical Infrastructure Security.

Sincerely,
Information Technology Sector Coordinating Council

Guy Copeland
Chairperson

Michael Aisenberg
Vice Chairperson

cc: The Honorable Gregory T. Garcia, Assistant Secretary for Cyber Security & Telecommunications, U.S. Department of Homeland Security

Members of the IT-SCC Executive Committee:

Guy Copeland, Computer Sciences Corporation, Chairperson
Michael Aisenberg, VeriSign, Vice Chairperson
Larry Clinton, Internet Security Alliance (ISA), Treasurer
Robert B. Dix, Jr., Juniper Networks, Inc., Acting Secretary
David Barron, BellSouth
Ken Watson, Cisco Systems, Inc.
Phil Reitinger, Microsoft Corporation
(Vacant), Unisys Corporation
Howard A. Schmidt, R & H Security Consulting LLC
Jerry Cochran, Information Systems Security Association (ISSA)
Liesyl Franz, Information Technology Association of America (ITAA)
James Bean, Verizon, Communications SCC Liaison

Designated Representatives of the IT-SCC Members:

Bell Security Solutions Inc.
BellSouth Corporation
CA, Inc
Center for Internet Security
Cisco Systems, Inc.
Computer and Communications Industry Association
Computer Sciences Corporation
Cyber Security Industry Alliance (CSIA)
Computing Technology Industry Association
EWA Information & Infrastructure Technologies, Inc.
Electronic Industries Alliance (EIA)
Entrust, Inc.
IBM Corporation
Information Systems Security Association (ISSA)
Information Technology Association of America (ITAA)
Intel Corporation
Information Technology - Information Sharing & Analysis Center (IT-ISAC)
International Systems Security Engineering Association (ISSEA)
Internet Security Alliance (ISA)
International Security Trust and Privacy Alliance (ISTPA)
KPMG LLP
Lockheed Martin
McAfee, Inc.
Microsoft Corporation
NTT America
R & H Security Consulting LLC
Seagate Technology
Symantec Corporation
U.S. Internet Service Provider Association (USISPA)
Unisys Corporation
VeriSign

Table of Contents

Executive Summary **1**

Sector Background and Goals 2

Risk Management 2

Develop and Implement Protective Programs 3

Information Sharing 3

CI/KR Protection Research and Development 4

Managing and Coordinating Sector Responsibilities 4

Implementing the SSP and Tracking Progress 4

Introduction and Purpose **5**

Document Organization 7

1. Sector Profile and Goals **9**

1.1 Definition 9

1.2 Scope 10

1.3 Sector Security Goals and Objectives 11

1.4 Partnering for Security 12

1.5 Authorities 15

1.6 Actions 15

1.6.1 Near Term (~1 year) 15

1.6.2 Long Term (1-3 years) 16

2. Risk Management **17**

2.1 Background of the IT Sector's Risk Environment 18

2.1.1 Various Entities' Risk Management Approaches 18

2.2 Developing an IT Sector Risk Profile 19

2.2.1 National IT Sector Risk Management Approach 20

2.3 Identifying Critical Functions 20

2.3.1 Screening and Assessing Consequences 20

2.3.2 Decomposing Critical IT Sector Functions 22

2.4 Assessing Threats, Vulnerabilities, Consequences, and Mitigations 22

2.4.1 Analyzing Threats 22

2.4.2 Assessing Vulnerabilities 23

2.4.3 Evaluating Consequences 24
2.4.4 Identifying Mitigations 24
2.5 Prioritizing for the IT Sector Risk Profile 25
2.6 Risk Management Information 26
2.7 Actions 27
2.7.1 Near Term (~1 year) 27
2.7.2 Long Term (1-3 years) 28
3. Develop and Implement Protective Programs 29
3.1 Current IT Sector Protective Programs 29
3.2 Identification and Implementation of New Protective Programs 31
3.2.1 Establish a Protective Program Working Group 31
3.2.2 Determine Needs and Capabilities 31
3.2.3 Identify Protective Actions 32
3.2.4 Develop an Implementation Plan 32
3.3 Protective Program Performance 32
3.4 Actions 33
3.4.1 Near Term (~1 year) 33
3.4.2 Long Term (1-3 years) 33
4. Information Sharing 35
4.1 Types of Information 35
4.2 Information Originators and Users 37
4.3 An Enhanced IT Sector Information Sharing Framework 39
4.3.1 Information Sharing Focal Points 40
4.3.2 Policies and Procedures for Sharing and Reporting Incidents 41
4.3.3 Procedures for Protecting and Disseminating Sensitive Proprietary Industry Information 41
4.3.4 Access to Classified and Sensitive But Unclassified (SBU) Government Information 42
4.3.5 Mechanisms for Communicating and Disseminating Information 43
4.4 Actions 43
4.4.1 Near Term (~1 year) 43
4.4.2 Long Term (1-3 years) 45
5. CI/KR Protection Research and Development 47
5.1 Current IT Sector Research and Development 47
5.2 IT Sector R&D Priorities 48
5.3 Coordinating IT Sector R&D Priorities 49
5.4 Actions 51
5.4.1 Near Term (~1 year) 51

5.4.2 Long Term (1-3 years) 51
6. Managing and Coordinating Sector Responsibilities 53
6.1 Program Management Approach 53
6.2 Processes and Responsibilities 53
6.2.1 SSP Maintenance and Update 53
6.2.2 Annual Reporting 53
6.2.3 Resources and Budgets 54
6.2.4 Training and Education 54
6.3 Roles and Responsibilities 56
6.3.1 Sector-Specific Agency 56
6.3.2 IT Sector Coordinating Council 57
6.3.3 IT Government Coordinating Council 57
6.3.4 Shared Cross-Sector Cyber Security Responsibilities 58
6.4 Actions 58
6.4.1 Near Term (~1 year) 58
6.4.2 Long Term (1-3 years) 58
7. Implementing the SSP and Tracking Progress 59
7.1 Tracking Progress Challenges 59
7.2 Measurement Overview 59
7.3 Measurement Approach 60
7.4 Goals and Objectives Measurement 60
7.5 Activities Implementation 62
7.6 Reporting on Progress 63
7.7 Actions 64
7.7.1 Near Term (~1 year) 64
7.7.2 Long Term (1-3 years) 64
Appendix 1: List of Acronyms and Abbreviations 65
Appendix 2: Authorities 69
Homeland Security/National Security IT Authorities 69
National Strategies 71
Management and Acquisition of Federal Government Information Technology 72
Information Technology Audit-Related Authorities 73
National Preparedness and Response Authorities Related to Information Technology 74
Information Technology Communications Related Authorities 74
Information Technology Privacy Authorities and Information Protection Related Authorities 74
International Standards and Guidelines 75

Appendix 3: Common Risk Management Frameworks 77
Appendix 4: IT Sector-Related Protective Programs 79
Appendix 5: Action Items 89

List of Figures

Figure 2-1. Developing the IT Sector Risk Profile 19
Figure 2-2. Notional Risk Priority Matrix 25
Figure 2-3. Risk Management Information 26
Figure 4-1. Information Flows 37
Figure 4-2. Notional Relationship Among Security Partners and Types of Information 39
Figure 7-1. IT Sector Measurement Approach 60
Figure 7-2. Notional Gantt Chart to Indicate Goal and Objective Implementation Progress at Q4 2008 61
Figure 7-4. Notional Gantt Chart to Indicate Activity Implementation Progress at Q4 2008 63

List of Tables

Table 1-1. Examples of IT Security Partners 14
Table 2-1. Critical IT Sector Functions and Descriptions 21
Table 3-1. Protective Program Capabilities that Support IT Sector Goals 30
Table 4-1. Types of Information Produced by Security Partners (Notional Template) 38
Table A4-1. Existing Protective Programs that Support the Overarching IT Sector Goals 79

Executive Summary

Information technology (IT) is central to our Nation's security, economy, and public health and safety. Businesses, governments, academia, and private citizens are increasingly dependent on IT Sector functions and services as are all other critical infrastructure sectors' products and services. The Sector has diverse global operations that are interdependent and interconnected with those of other infrastructure sectors. These operations face numerous, multifaceted, global threats every day. Individual IT Sector entities proactively manage risk to their own operations and those of their customers,[1] through constant monitoring and mitigation activities designed to prevent daily incidents from becoming significant disruptions to national security, the economy, and public health and safety. Although the IT infrastructure has a certain level of inherent resilience, its interdependent and interconnected structure presents challenges and opportunities for coordinating public and private sector preparedness activities.

> Daily protective activities by individual sector entities to prevent, protect against, and mitigate threats and disruptions contribute to the sector's overall steady state of preparedness. This plan focuses on public and private sector planning to enhance the ability of the sector as a whole to prevent, protect against, mitigate, and respond to nationally significant events, technological emergencies, and Presidentially-declared disasters that threaten, disrupt, or cripple IT Sector infrastructure.

Various efforts championed by the public and private sectors have been undertaken to address infrastructure protection and cyber security. The Homeland Security Act of 2002 required the first-ever all-encompassing coordinated national critical infrastructure and key resources (CI/KR) protection effort. Homeland Security Presidential Directive 7 (HSPD-7) identifies 17 CI/KR sectors, including the IT Sector, and requires Federal agencies, coordinated by the Department of Homeland Security (DHS), to identify, prioritize, and coordinate the protection of the Nation's critical infrastructure. The National Infrastructure Protection Plan (NIPP) and its complementary Sector-Specific Plans (SSP) provide a consistent, unifying structure for integrating existing and future CI/KR protection efforts. They also provide the core processes and mechanisms to enable government and private sector security partners to work together to implement CI/KR protection initiatives.

Public and private sector security partners have an enduring interest in assuring the availability of the infrastructure and promoting its resilience. The IT SSP represents an unprecedented partnership and collaboration between the IT public and private sectors to address the complex challenges of CI/KR protection. Public and private sector organizations each represent and bring unique capabilities to the partnership, and derive value from the exchange. Successful CI/KR protection is the commitment of IT Sector public and private sector security partners to share information and provide the tools and capabilities necessary for an effective partnership.

[1] As determined by contracts with those customers

The IT SSP was collaboratively developed by DHS' National Cyber Security Division (NCSD) as the Sector Specific Agency (SSA) for the IT Sector and sector security partners, including the IT Sector Coordinating Council (SCC) and IT Government Coordinating Council (GCC). The IT SSP is a planning document that provides guidance on how public and private partners will work together to protect IT Sector CI/KR. It does not provide specific procedures for individual Sector entities' operations and is not designed to guide Federal or State government efforts to respond to events. For the purposes of the IT SSP, "response" refers to individual entity activities as well as joint public and private sector activities, to position the Sector to ensure that any disruptions or manipulations of the IT infrastructure are brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States. Federally coordinated response, including activities addressed by the National Response Plan, will be specifically referenced as such. Although this document is the first jointly developed IT SSP, it will not be the last. Threats and vulnerabilities are continually evolving, and consequently plans and programs for addressing these must evolve accordingly.

Sector Background and Goals

The IT Sector is composed primarily of virtual and distributed functions necessary to provide IT products and services. These critical IT Sector functions are provided by a combination of entities—often owners and operators and their respective associations—that provide hardware, software, IT systems, and services. These entities maintain and reconstitute the network, including the Internet. The Internet encompasses the global infrastructure of packet-based networks and databases that use a common set of protocols to communicate. The networks are connected by various transports, and the availability of these networks and services is the collective responsibility of the IT and Communications Sectors.

IT Sector Goals

- Prevention and Protection Through Risk Management
- Situational Awareness
- Response, Recovery, and Reconstitution

The IT SSP provides a framework for identifying and managing Sector risk during the steady-state (i.e., routine day-to-day business operations) to prevent, protect against, mitigate, and prepare for nationally significant events, including those cyber or physical events, technological emergencies, or Presidentially- declared disasters, that threaten, disrupt, or cripple the IT Sector infrastructure. Public and private sector security partners have collaborated to identify overarching goals for the sector that are intended to ensure overall Sector preparedness. Pursuit of these goals requires individual actions by a wide array of public and private security partners.

Risk Management

Public and private sectors are collaborating to address risks that could affect the ability of the Sector's critical functions to support the economy and national security. Given the IT Sector's complex and global operations and the diverse and interconnected nature of its supporting infrastructure, the Sector is using a qualitative, top-down approach that considers the Sector security goals and objectives and then identifies critical Sector functions. The resulting sector-wide risk approach described in the IT SSP addresses the three factors of risk as described in the NIPP—threat, vulnerability, and consequence—and focuses on those IT functions with national consequence. Many enti-

IT Sector Critical Functions

- Provide IT Products and Services
- Provide Incident Management Capabilities
- Provide Domain Name Resolution Services
- Provide Identity Management and Associated Trust Support Services
- Provide Internet Based Content, Information, and Communications Services
- Provide Internet Routing, Access and Connection Services

ties have robust risk management activities in place. As such, the IT SSP does not provide guidance for individual entities' risk management activities. Coordination of risk management activities by IT Sector security partners should help focus efforts and resources on ensuring the continued availability of critical IT Sector functions, products, and services and improved resilience of the nationally critical IT infrastructure.

The IT Sector approach to risk assessment consists of three steps: (1) identifying critical functions; (2) assessing threats, vulnerabilities, consequences, and mitigations; and (3) assessing and prioritizing risks. Critical IT Sector functions are identified and evaluated using consequences to focus on only those that meet certain thresholds for national significance. By defining critical IT Sector functions during development of the IT SSP, the IT Sector has completed the first step of the risk assessment approach.[2] The IT Sector will then apply threats to their critical functions to identify vulnerabilities. An all-hazards approach that addresses the spectrum of natural and manmade threats will be used. The IT Sector will complement the traditional threat assessment approach with additional factors based on capabilities and intent independent of known actors to consider emerging non-traditional threats. Vulnerabilities for critical functions and their applicable specific threat scenarios will be identified and assessed, along with mitigations that reduce specific risk factors.

Using HSPD-7 consequence categories and criteria for evaluating nationally significant events, the IT Sector's approach to consequence assessment identifies impacts on national and economic security and public health, safety, and confidence resulting from the disruption or degradation of a critical function. Consistent measurements will be used to evaluate threat, vulnerability, and consequence and enable the comparison of risks across the sector. The outcome of the national IT Sector risk assessment will be a prioritization of sector risks according to consequence and likelihood. The IT Sector will focus primarily on risks with high consequence and high likelihood.

Develop and Implement Protective Programs

Protective programs include measures or activities that are undertaken by various security partners to prepare for, prevent, protect, respond to, and recover from incidents that have the potential to impact critical IT Sector functions. Current protective programs provide capabilities for reducing vulnerabilities, analyzing threat, sharing information, and managing and responding to incidents. During the initial SSP development process, IT SCC and IT GCC members identified existing protective programs and areas where new programs or enhanced capabilities are needed, including robust coordinated response capabilities; reconstitution of data, communication services, and networks; out-of-band data delivery capability; and cyber grants for State governments.

The IT Sector will determine additional protective program needs identified through the risk management process. This process will be used to address those needs in which no viable private sector solution exists for meeting the need or high transaction costs or legal barriers would cause significant coordination and/or implementation challenges.

Information Sharing

Information sharing is a key element to fulfilling the overarching goals of the IT Sector and implementing the NIPP framework. Information sharing enables owners and operators, decision makers, managers, and others to detect, deter, and prevent attacks and incidents; identify trends; assess risks; provide warnings to help mitigate impacts; and coordinate response activities. IT Sector public and private sector security partners are focused on building and maintaining trusted relationships based on the simple premise that, for information to be useful, it must be shared with the right people at the right time. The IT Sector's approach focuses on sharing information between and among the government and those individuals who operate, administer, and own the IT infrastructure.

[2] These are public and private sector consensus critical IT Sector functions for Government Fiscal Year 2007. Annual planning enables the review and update of these functions to reflect changes in the IT Sector environment.

The IT Sector envisions an enhanced information sharing framework that identifies key focal points for policy and operational information sharing, processes, and procedures, and ways to facilitate access to information. The IT Sector's vision for an ideal or future state of information sharing includes policy, cultural, organizational, and technological conditions that facilitate two-way, decentralized, yet coordinated information sharing.

CI/KR Protection Research and Development

In recent years, numerous committees and organizations have analyzed and reported on IT Sector security gaps. The result is a substantial body of work describing these gaps and proposing research and development (R&D) priorities to bridge them. The IT Sector leveraged this work to identify IT Sector R&D priorities based on the common themes established by prior analyses.

Addressing R&D priorities requires engaging multiple partners to pool resources to raise awareness and increase coordination. Establishment of an online clearinghouse for exchanging information and collaborating on IT Sector R&D priorities and conducting an annual IT Sector R&D workshop may provide mechanisms for outreach, review of research projects, consideration of gaps in the execution of national research priorities, and reaching consensus on general government and private sector requirements. In addition, a common taxonomy for exchanging information on progress toward accomplishing the sector's goals for each R&D priority can promote understanding across the IT Sector and further collaboration.

IT Sector R&D Priorities

- Cyber Situational Awareness and Response
- Forensics
- Identity Management: Authentication, Authorization, and Accounting
- Intrinsic Infrastructure Protocols Security
- Modeling and Testing
- Control Systems Security
- Scalable and "Composable" Secure Systems
- Secure Coding, Software Engineering, and Hardware Design Improvement
- Trust and Privacy

Managing and Coordinating Sector Responsibilities

As described in HSPD-7, the DHS is responsible for managing and coordinating IT Sector CI/KR protection activities, including leading the development of an SSP for the IT Sector. Within the department, this responsibility has been delegated to NCSD. Sector responsibilities include maintenance and update of the SSP, annual reporting, resources and budgets, and training and education. Public and private sector security partners have common and unique roles and responsibilities.

Implementing the SSP and Tracking Progress

Tracking the progress of implementing the actions set forth in this plan is essential to the SSP's success. A collaborative and iterative process that benefits from the voluntary input of the IT SCC and IT GCC members can track the SSP's implementation most accurately and provide public and private sector security partners with a shared understanding of progress toward achieving the sector's goals.

Implementing and tracking the action items in support of the sector's goals and objectives requires commitment and resources (e.g., financial, time, personnel, and expertise) from the public and private sectors. Public and private sector security partners will need to prioritize the actions in this plan and proceed with implementation and tracking using an iterative approach while taking into account resource availability.

Introduction and Purpose

Information technology (IT) is central to our Nation's security, economy, public health, and safety. The IT Sector accounts for about 7 percent of the U.S. gross domestic product.[3] On a daily basis, more than $3 trillion worth of economic activity (e.g., securities sales settlements, check clearances, and interbank transfers) passes over secure Federal financial networks.[4] IT systems enable this economic activity, which is essential to maintaining homeland and national security. Critical infrastructure and key resources (CI/KR) sectors rely on the IT Sector for products and services, including the reliable operation of networks and systems and the movement and storage of critical data. Conversely, the IT Sector relies on many other sectors, including the Energy and Communications Sectors, for daily operations.

The Sector has diverse global operations that are interdependent and interconnected with those of other infrastructure sectors. These operations face numerous multifaceted global threats daily. Individual IT Sector entities proactively manage risk to their own operations and those of their customers,[5] through constant monitoring and mitigation activities designed to prevent daily incidents from becoming significant disruptions to national security, the economy, and public health and safety. Although the IT infrastructure has a certain level of inherent resilience, its interdependent and interconnected structure presents challenges and opportunities for coordinating public and private sector preparedness activities.

Since the 1990s, the public and private sectors have been working to address these challenges and opportunities. In 1997, a Presidential Commission identified the risks to critical infrastructures in a seminal public report, *Critical Foundations: Protecting America's Infrastructures*. Year 2000 initiatives and Executive Order 13231[6] also made cyber security a priority, subsequently increasing funds available to secure Federal networks. Following the terrorist attacks of September 11, 2001, the Homeland Security Act of 2002 required the first comprehensive coordinated national CI/KR protection effort. The President's National Strategy to Secure Cyberspace articulates five national priorities for protecting against a debilitating disruption of the operation of information systems as part of national CI/KR protection efforts. In 2003, President George W. Bush issued Homeland Security Presidential Directive 7 (HSPD-7) requiring Federal agencies, coordinated by the Department of Homeland Security (DHS), to identify, prioritize, and coordinate the protection of CI/KR for the purposes of preventing, deterring, and mitigating the effects of deliberate efforts to destroy, incapacitate, or exploit them. Implementing this policy requires substantial commitment to public-private partnership. The directive identifies 17 CI/KR, including the IT Sector, and pairs each CI/KR sector with a sector-specific agency (SSA) for partnering on protective initiatives. HSPD-7 requires DHS to develop an overall National Infrastructure Protection Plan (NIPP) and specifically assigns DHS the mission of establishing uniform policies, approaches,

[3] World Information Technology and Services Alliance, *Digital Planet 2006: The Global Information Economy*, May 2006, www.witsa.org/digitalplanet/2006/DP2006_ExecSummary.pdf.
[4] Federal Reserve Board, "Telling the Fed's Story through Money in Motion," www.phil.frb.org/publicaffairs/pubs/ar03telling.pdf.
[5] As determined by contracts with those customers.
[6] Executive Order 13231, Critical Infrastructure Protection in the Information Age, October 2001.

guidelines, and methodologies for integrating infrastructure protection and risk management activities within and across sectors, along with developing metrics and criteria for related programs and activities.

The NIPP and its complementary Sector-Specific Plans (SSP) provide a consistent, unifying structure for integrating existing and future CI/KR protection efforts. They also define the core processes and mechanisms for public and private sector security partners[7] to implement coordinated CI/KR protection initiatives. Implementation of the NIPP, its complementary SSPs, the National Response Plan (NRP), and the National Incident Management System (NIMS) define readiness targets, priorities, standards for assessment, strategies, and a system for assessing the Nation's overall preparedness across four mission areas: prevention, protection, response, and recovery.

Public and private sector security partners have an enduring interest in assuring the availability of the infrastructure. The IT Sector's market-based environment enables rapid innovation and drives investments in security to meet customers' changing needs and promote the resilience of the IT Sector. Prevention and protection through risk management, situational awareness, and response, recovery, and reconstitution efforts are most effective when full participation of public and private sector security partners exists; such efforts suffer without the full participation of either partner.

The IT SSP represents an unprecedented partnership and collaboration between the IT public and private sectors as they leverage their unique capabilities to address the complex challenges of CI/KR protection. The IT Sector entities involved in development of the SSP believe that its implementation will provide value for the sector and customers who rely on its products and services. As such, IT Sector entities involved in development of the SSP will work to convey the national security and business value for participation in SSP implementation activities to other members of the IT Sector.

IT private sector entities have a comprehensive understanding of critical IT Sector functions, capabilities, and infrastructure. This understanding enables the private sector to leverage existing information sharing mechanisms and its insights into risk mitigation and best practices to improve the Sector's security posture in a reasonable, feasible, and practical manner. Private sector entities manage risk to their business operations, voluntarily implement protective initiatives designed to enhance their steady-state physical, human, and cyber security, and manage response to day-to-day incidents to prevent and prepare for significant events. Individual private sector capabilities are also essential for incident management, as well as response, recovery, and reconstitution of essential government functions. Because the private sector can quickly focus on requirements and needs, it often takes the lead in developing and deploying innovative solutions, increasing the skills and availability of security professionals, and developing products and services that are responsive to the rapidly changing threat environment.

Federal Government coordination and leadership of IT Sector CI/KR protection efforts is justified and, in certain instances, required. For example, continuity of government (Federal, State, and local) requires ensuring the security and availability of governments' cyber and physical infrastructure necessary to support their essential missions and services. To fully leverage the unique capabilities of the private sector, the Federal Government is working to ensure that the private sector is engaged, as early as possible, in the development, implementation, and maintenance of initiatives and policies regarding ownership and operation of the private sector's products, services, and systems. In addition, government has a role to play in instances where high transaction costs or legal barriers lead to significant coordination problems, where government operations exist in the absence of private sector forces, or where critical shared resources are under provisioned. The public sector can create a legal and regulatory environment that stimulates and facilitates voluntary private sector efforts to improve security, including establishing the policies and protocol needed to share timely analytical and useable information about threats to the IT Sector. Finally, the public sector sponsors efforts such as cross-sector interdependency studies, research and development (R&D) into the security of basic Internet protocols, and research studies on return on investment (ROI) for businesses that undertake risk management efforts and implement improved security processes and tools.

[7] The term "security partners" refers to the stakeholders in the NIPP planning process. These stakeholders include all government levels (Federal, State, Territorial, regional, local, and tribal), regional organizations, international partners, and private sector owners and operators.

Information sharing among and between public and private sector security partners is essential for achieving security. Through improved information sharing and analysis, the public and private sectors will be better equipped to identify threats and vulnerabilities, and to exchange mitigating and preventive tactics and resources to address them. Successful CI/KR protection requires the commitment of public and private IT Sector security partners to provide tools and capabilities for an effective partnership. Only with robust exchanges and rigorous critique and evolution of the sector's goals and priorities will the value proposition continue to be realized.

The IT SSP was developed collaboratively by IT Sector security partners, including representatives from the DHS's National Cyber Security Division (NCSD), the IT Sector Coordinating Council (SCC), and the IT Government Coordinating Council (GCC). The SSP is a planning document that focuses on meeting sector goals that are most pressing for homeland, economic, and national security purposes and identifies actions (current, near term, and long term) for steady-state preparedness, including prevention and protection of critical IT Sector functions that enable sector response and recovery activities. The SSP does not provide specific procedures for individual IT Sector entities' operations. The SSP:

- Outlines the IT Sector security partners' joint implementation of the NIPP risk management framework by describing an approach for identifying, assessing, prioritizing, and protecting critical IT Sector functions;
- Establishes shared IT Sector goals and objectives and aligns initiatives to meet them;
- Describes roles, responsibilities, and opportunities that NCSD, IT SCC, IT GCC, and other security partners can play in implementing the SSP; and
- Provides opportunities for integrating public and private sector preparedness efforts with tools and technologies essential for effective incident response, system remediation, and reconstitution under the NRP and NIMS.

Although this document is the first jointly developed IT SSP, it will not be the last. Threats and vulnerabilities evolve continually, and consequently plans and programs for addressing them must evolve accordingly. Annual planning enables public and private sectors to reassess priorities and realign resources to meet changing needs.

Document Organization

The organization of the IT SSP represents a consensus outline based on IT SCC and IT GCC input. The following provides a mapping between the consensus outline and the SSP outline provided in the 2006 CI/KR Protection SSP Guidance to facilitate review by readers familiar with that format.

- **Section 1: Sector Profile and Goals.** Maps to SSP Guidance, Chapter 1: Sector Profile and Goals.
- **Section 2: Risk Management.** Maps to SSP Guidance, Chapter 2: Identify Assets, Systems, Networks, and Functions; Chapter 3: Assess Risk; and Chapter 4: Prioritize Infrastructure.
- **Section 3: Develop and Implement Protective Programs.** Maps to SSP Guidance, Chapter 5: Develop and Implement Protective Programs
- **Section 4: Information Sharing.** Maps to SSP Guidance, Chapter 8, Section 8.4, Information Sharing and Protection.
- **Section 5: CI/KR Protection Research and Development.** Maps to SSP Guidance, Chapter 7: CI/KR Protection Research and Development.
- **Section 6: Managing and Coordinating Sector Responsibilities.** Maps to SSP Guidance, Chapter 8: Managing and Coordinating SSA Responsibilities.
- **Section 7: Implementing the SSP and Tracking Progress.** Maps to SSP Guidance, Chapter 8: Measure Progress.

Each SSP section also includes two consistent elements—a callout box discussing the value proposition for public and private sector security partners and near- and long-term actions. Near-term (~1 year) and long-term (1-3 years) actions often have component subactions and may be tracked at that level through implementation. Appendix 5 summarizes the IT SSP actions. Although each near-term action may not be completed within the next year, it is expected that progress toward completing the action will occur within the next year (i.e., 2007-2008).

1. Sector Profile and Goals

This section describes the IT Sector, identifies the IT SSP's focus, establishes the sector's goals, and describes IT Sector security partners' roles and responsibilities.

1.1 Definition

Critical IT Sector functions support the Sector's ability to produce and provide high assurance IT products and services for a variety of sectors. Through the IT SSP development process, the Sector identified six critical functions:

- provide IT products and services;
- provide incident management capabilities;
- provide domain name resolution services;
- provide identity management and associated trust support services;
- provide Internet-based content, information, and communications services; and
- provide Internet routing, access and connection services.

These functions are distributed across a broad network of infrastructure, managed on a proactive basis and therefore able to withstand and rapidly recover from most threats.[8]

> The Internet encompasses the global infrastructure of packet-based networks and databases that use a common set of protocols to communicate. The networks are connected by various transports. The availability of the network and its services is the collective responsibility of the IT and Communications sectors.

These critical IT Sector functions are provided by a combination of entities—often owners and operators and their respective associations—who provide hardware, software, IT systems, and services. IT services include development, integration, operations, communications, and security. IT Sector entities include the following:[9]

- Domain Name System (DNS) root and Generic Top-Level Domain (GTLD) operators;
- Internet service providers (ISPs);
- Internet backbone providers;
- Internet portal and e-mail providers;

[8] Threat is defined as the intention and capability of natural or manmade (intentional or unintentional) events that would be detrimental to the IT Sector. This definition was developed by the IT Sector based on the terms and definitions in the NIPP.

[9] Operating Charter of the Information Technology Sector Coordinating Council, January 24, 2006 https://www.it-isac.org/documents/itscc/index.php

- Networking hardware companies (e.g., fiber-optics makers and line acceleration hardware manufacturers) and other hardware manufacturers (e.g., personal computer (PC) and server manufacturers and information storage);
- Software companies;
- Security services vendors;
- Communications companies that characterize themselves as having an IT role;
- Edge and core service providers;
- IT system integrators; and
- IT security associations.

In addition, Federal, State, and local governments are a component of the IT Sector as providers of government IT services that are designed to meet the needs of citizens, businesses, and employees. The IT Sector includes public and private sector entities.

1.2 Scope

The IT SSP provides a framework for identifying and managing risk during steady-state (i.e., routine day-to-day) business operations to prevent, protect against, mitigate, and prepare for nationally significant events; technological emergencies; or presidentially declared disasters that threaten, disrupt, or cripple IT Sector infrastructure. Specifically, the IT SSP is concerned with all hazard events with cyber or physical consequences that:

- Cause, or are likely to cause, harm to mission-critical functions across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, information systems, services, or networks; and/or
- Threaten public health or safety, undermine public confidence, have a negative effect on the national economy, or diminish the security posture of the Nation.

Such nationally significant events likely would affect communications and/or IT services in at least one region and possibly several regions of the country, including at least one major metropolitan area. Events would involve multiple communications service providers and/or IT products and services, resulting in a significant degradation of other essential infrastructures. Such an event would have an impact on the availability and integrity of communications and IT services for at least a significant portion of a business day or longer.[10]

Roles and Responsibilities

Private Sector:

- Own, operate, and provide IT Sector critical functions;
- Monitor IT Sector critical functions for abnormal events;
- Alert United States Computer Emergency Readiness Team (US-CERT) and others to any events that potentially threaten, disrupt, or cripple IT Sector infrastructure; and
- Work with the National Cyber Response Coordination Group (NCRCG) as appropriate to consider the implications of the event.

Government:

- Own, operate, and provide IT Sector critical functions (as applicable);
- Monitor government networks and systems for abnormal events;
- Alert US-CERT to any events that potentially threaten, disrupt, or cripple IT Sector infrastructure;
- Provide information to the NCRCG for its consideration; and
- Make a recommendation regarding whether an event involving cyber is nationally significant.

[10] The discussion of the type of events that the IT SSP is concerned with is consistent with the NCRCG's Working Definition of a Cyber Incident of National Significance, December 2006. The NCRCG, a forum of 13 government agencies, coordinates intragovernmental and public-private preparedness and operations to respond to and recover from cyber incidents of national significance. The NCRCG is a key cyber incident management body that provides strategic assessments and ensures that appropriate Federal resources and capabilities are deployed to ensure an adequate response.

Identification of the scope of events that are of concern to the IT Sector is an important element of government and private sector efforts to identify, prioritize, and protect critical IT Sector functions. It provides a foundation for addressing overall preparedness, including prevention and protection under the IT SSP and understanding when to transition to Federally-coordinated response[11] and recovery under the NIMS and NRP.

1.3 Sector Security Goals and Objectives

Vision Statement for the Information Technology Sector

Public and private IT Sector security partners will continue building infrastructure resilience to support:

- *The Federal Government's performance of essential national security missions and preservation of general public health and safety;*
- *State and local governments' abilities to maintain order and to deliver minimum essential public services; and*
- *The orderly functioning of the economy.*

The IT Sector will continue to coordinate with other CI/KR sectors and work to ensure that any disruptions or manipulations of critical IT Sector functions are brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States.

Public and private sector security partners collaborated to identify overarching Sector goals that support efforts to prevent, prepare for, protect against, mitigate, respond to, and recover from nationally significant events. These goals create a mutually beneficial framework to develop risk management and protective strategies that will enhance sector security. Pursuit of these goals requires action by a wide array of public and private security partners, including the commitment of expertise and the identification and prioritization of resources. IT Sector security partners will review these goals and progress toward implementing them annually. The goals and their associated objectives are described below in no particular order.

Goal 1: Prevention and Protection Through Risk Management. Identify, assess, and manage risks to the IT Sector's infrastructure and its international dependencies.

- **Objective 1.1:** Identify and annually review[12] critical IT Sector functions that support the Nation's security, economy, public health, and safety.
- **Objective 1.2:** Assess and prioritize risks to critical IT Sector functions, including evaluating emerging threats, vulnerabilities, and technology, and mapping them against the infrastructure to prioritize protective efforts.
- **Objective 1.3:** Tailor protective measures, which mitigate associated consequences, vulnerabilities, and threats, to accommodate the diversity of the IT Sector and develop and share IT security best practices and protective measures with security partners.
- **Objective 1.4:** Encourage IT Sector entities to exchange information about risk management strategies and foster a better understanding of how they improve the overall posture of the sector.

[11] For the purposes of the IT SSP, response refers to individual public and private sector entity and joint public and private sector activities to position the Sector to ensure that any disruptions or manipulations of the IT infrastructure are brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States. Federally coordinated response will be specifically referenced as such.

[12] Critical IT Sector functions will be reviewed annually to determine if technological and environmental changes have occurred that alter the set of functions or their descriptions.

Goal 2: Situational Awareness. Improve situational awareness during normal operations, potential or realized threats and disruptions, intentional or unintentional incidents, crippling attacks (cyber or physical) against IT Sector infrastructure, technological emergencies and/or failures, or presidentially declared disasters.

- **Objective 2.1:** Collaborate, develop, and share appropriate threat and vulnerability information among public and private sector security partners, including development of indications and warnings.
- **Objective 2.2:** Expand strategic analytical capabilities that facilitate public and private sector security partner collaboration to identify potential incidents.

Goal 3: Response, Recovery, and Reconstitution. Enhance the capabilities of public and private sector security partners to respond to and recover from realized threats and disruptions, intentional or unintentional incidents, crippling attacks (cyber or physical) against IT Sector infrastructure, technological emergencies and/or failures, or presidentially declared disasters, and develop mechanisms for reconstitution.

- **Objective 3.1:** Develop and maintain communications, including establishing mechanisms and processes for communicating with other sectors during contingencies, and conduct annual tests of the resulting communication plans and programs.
- **Objective 3.2:** Develop and maintain incident response and coordination plans and procedures, and exercise them annually to ensure readiness and resilience.
- **Objective 3.3:** Develop plans, protocols, and procedures to ensure that critical IT Sector functions can be reconstituted rapidly after an incident.
- **Objective 3.4:** Collaborate with law enforcement to identify and mitigate criminal activities that have the potential to harm the sector's infrastructure.

1.4 Partnering for Security

As set forth in the NIPP, the sector partnership model[13] encourages the public and private sectors to collaborate on their respective CI/KR protection activities. This collaboration is accomplished through SCCs and GCCs, which form a national framework for coordinating CI/KR protection within and across sectors.

IT GCC Membership (as of December 2006)	
Department of Commerce • National Institute of Standards and Technology (NIST) • National Technology and Information Administration Department of Defense/Office of the Assistant Secretary of Defense for Networks and Information Integration Department of Homeland Security • Preparedness Directorate/NCSD (IT GCC Chair) • Preparedness Directorate/Office of Infrastructure Protection • Preparedness Directorate/(National Communications System (NCS) • Science and Technology Directorate	Department of Justice Department of State Department of the Treasury Office of the Director of National Intelligence Office of Management and Budget (OMB) Metropolitan Information Exchange National Association of State Chief Information Officers

[13] For additional information on the Sector Partnership Model, see section 4 of the NIPP.

IT SCC Membership (as of December 2006)		
BearingPoint	EWA Information and Infrastructure Technologies, Inc.	KPMG LLP
Bell Security Solutions, Inc.	IBM Corporation	Lockheed Martin
BellSouth Corporation	Information Systems Security Association	McAfee, Inc.
Center for Internet Security	Information Technology Association of America	Microsoft Corporation
Cisco Systems, Inc.	Information Technology Information Sharing and Analysis Center	NTT America
CA International, Inc.	Intel Corporation	R&H Security Consulting, LLC
Computer and Communications Industry Association	International Systems Security Engineering Association	Seagate Technology
Computer Sciences Corporation	Internet Security Alliance	Symantec Corporation
Computing Technology Industry Association	Internet Security Systems, Inc.	System 1, Inc.
Cyber Security Industry Alliance	Internet Security Trust and Privacy Allicance	TestPro
Electronic Industries Alliance	Juniper Networks, Inc.	Unisys Corporation
Entrust, Inc.		U.S. Internet Service Provider Association
		VeriSign
		Verizon

The IT SCC (composed of IT industry members) and the IT GCC (composed of government representatives) are the primary bodies for communicating their respective public and private perspectives and for developing collaborative policies, strategies, and security efforts to advance CI/KR protection. SCC and GCC representatives share experiences, ideas, best practices, and innovative approaches related to CI/KR protection and risk management for their respective sectors. In March 2006, the DHS established the Critical Infrastructure Partnership Advisory Council (CIPAC) to facilitate coordination and dialogue between the SCCs and GCCs. The various SCCs address cross-sector issues and interdependencies through their participation in the Partnership for Critical Infrastructure Security (PCIS). The IT SCC will coordinate with other sectors on cross-sector issues, such as cyber security, through forums such as the PCIS.

To achieve an integrated national plan, the DHS must coordinate with all security partners that have equities or interests in CI/KR protection. Public and private sector security partners are crucial not only to the implementation of this plan but also to the broader policy and operational relationships that enhance the IT Sector's overall security posture. Table 1-1 provides examples of IT security partners.

Table 1-1: Examples of IT Security Partners

Security Partner	Description
Office of Cyber Security and Communications	The office works to ensure the security, resilience, and reliability of the Nation's cyber and communications infrastructure in collaboration with the public and private sectors. The office is composed of the NCSD and the NCS. The DHS is designated as the SSA for the IT Sector. That responsibility is delegated to NCSD, which is responsible for coordinating with other government departments and agencies (through the IT GCC) and the private sector (through the IT SCC) to develop and implement the IT SSP.[14] The DHS also is designated as the SSA for the Communications Sector, with that responsibility delegated to NCS.
IT Government Coordinating Council	Chaired by NCSD and established in April 2005, the IT GCC collaborates with the IT SCC to plan, implement, and execute sector-wide security programs for the Nation's IT critical infrastructure.
Other Federal Departments and Agencies	The responsibilities of other Federal departments and agencies are distinct from the SSA's responsibilities. For example, under the Federal Information Security Management Act, the OMB and the NIST have responsibility for overseeing the security of, and providing guidance for, the Federal Government's IT assets, systems, networks, and functions. Federal law enforcement agencies, such as the Federal Bureau of Investigation (FBI), play a critical role in investigating threats and prosecuting the perpetrators of cyber and physical crimes. The intelligence community (IC) uses national-level intelligence capabilities and resources to identify and counter threats. Law enforcement and the IC provide early warning or potential target information that can help the IT Sector and homeland security community implement preventive and protective measures.
State and Local Governments	State and local governments provide IT services that fulfill the needs of their citizens, businesses, and employees. The National Association of State Chief Information Officers (NASCIO), which represents the senior IT leaders for each State, is a key security partner of the IT Sector. State government participation in the IT SSP is achieved through the representation of NASCIO on the IT GCC. Local government participation in the IT SSP is achieved through the representation of the Metropolitan Information Exchange on the IT GCC.
IT Sector Coordinating Council	Established in January 2006, the IT SCC addresses policy and strategy issues and advises government counterparts on sector CI/KR protection issues. The IT SCC is self-organized, self-run, and self-governed. It enables owners and operators to coordinate on a wide range of sector-specific strategies, policies, activities and issues.[15]
IT-ISAC	The IT Information Sharing and Analysis Center (IT-ISAC) offers its private sector members a current and coherent picture of the security posture of the IT infrastructure.[16] In addition to these policy coordination bodies, the IT Sector also relies on the IT-ISAC to provide operational and tactical capabilities for sharing information.
Private Sector Owners and Operators	Owners and operators of IT CI/KR implement infrastructure protection practices as part of their routine business risk management activities and play a crucial role in the security of the IT Sector.
Communications Sector	Recognizing the growing convergence of IT and communications and their significant interdependencies, the IT Sector coordinates closely with the Communications Sector.[17] Partnering with the Communications Sector is especially important for exchanging information about the Internet infrastructure, a responsibility shared by both sectors.
Other CI/KR	IT Sector security partners understand how consumers use their products and services and recognize the cyber security challenges that they face. Although the cyber security practices for specific CI/KR are best addressed within their respective sectors, IT Sector security partners coordinate and work with other sectors to articulate and address the interdependence among the infrastructures as part of managing IT Sector risks.

[14] For additional information about the roles and responsibilities of the IT SSA, see section 6.
[15] For additional information about the roles and responsibilities of the IT SCC, see section 6.
[16] For additional information on the IT-ISAC, see section 4.
[17] Commonalities across both sectors' membership facilitate the coordination.

Security Partner	Description
Other ISACs	ISACs provide a trusted mechanism for information sharing within and among CI/KR. The National Coordinating Center (NCC) for Telecommunications, as the ISAC for the Communications Sector, is a well-established information-sharing center with a 24 hours per day, 7 days per week (24/7) operations center for monitoring threats and exchanging information between Communications Sector members and other interdependent critical infrastructure sectors (e.g., IT Sector). The Multi-State ISAC (MS-ISAC) provides a mechanism for information sharing and outreach to State and local governments regarding cyber security issues.[18]
Foreign Governments and International Organizations	Because the IT Sector is global in nature, interconnected, and interdependent, international partners play a key role in the prevention, protection, response, and recovery of critical IT Sector functions. Establishing and maintaining consistent and reliable relationships with international partners is vital to ensuring the security of the sector.

1.5 Authorities

Authorities addressing such issues as homeland security, national security, privacy, and IT audits affect or influence the IT Sector and provide direction to public and private sector security partners. Because of the interconnectedness of the IT and Communications Sectors, many authorities applicable to telecommunications are relevant to IT as well. Key authorities address the availability, resilience, and security of the infrastructure.

Appendix 2 presents an overview of key authorities that provide the foundation for IT Sector policies and regulations in the United States and guidance on sector coordination. These authorities—some of which apply to the Federal Government and others to the private sector—govern the collection, sharing, and protection of information, conduct of vulnerability and risk assessments, and the identification, development, and implementation of protective strategies and programs.

1.6 Actions

The following bulleted list includes near term and long term actions to be completed to implement this section of the SSP.

1.6.1 Near Term (~1 year)

- Facilitate the development of and articulate for IT Sector members the national security and business value for participation in SSP implementation activities. (*NCSD, SCC, and GCC*)
- Develop criteria that may be used for determining nationally significant events. (*NCSD, SCC, GCC, and NCRCG*) (*Underway*)
- Provide input into national-level efforts to clarify the roles and responsibilities of public and private sectors in Federally coordinated response, recovery, and reconstitution efforts involving nationally significant events. (*NCSD, SCC, GCC, and NCRCG*)
- Provide public and private sector perspectives and input to assist in planning for Federally coordinated response and recovery efforts involving nationally significant events. (*NCSD, SCC, GCC, and NCRCG input*)

[18] See section 4 for additional information about the MS-ISAC and its relationship to the IT Sector.

1.6.2 Long Term (1-3 years)

- Conduct exercises that test the implications of a nationally significant event and the resulting public and private sector roles, responsibilities, and capabilities. *(NCSD, SCC, GCC, and NCRCG)*
- Annually review and revise IT SSP goals, objectives, and authorities. *(GCC and SCC)*
- Hold joint IT and Communications sectors meeting biannually to address issues of interest to both sectors, and discuss potential areas for collaboration. *(NCSD, NCS, SCC, GCC, Communications SCC, and Communications GCC)*
- Work in partnership through the PCIS with the Communications Sector to help other CI/KR understand their dependence on the IT and Communications Sectors. *(NCSD, NCS, SCC, GCC, Communications SCC, and Communications GCC)*

2. Risk Management

Individual IT Sector entities routinely manage a wide range of risks to ensure the delivery of products and services to support their customers. Despite these individual entities' efforts, there is not yet a national-level understanding of risk faced by the IT Sector. Public and private sectors are collaborating to address these broader risks that could affect the ability of the sector's critical functions to support the economy and national security. The sector-wide risk approach describes how risk will be evaluated across the IT Sector focusing on critical IT Sector functions; it is not guidance for individual entities' risk management activities. A sector-wide risk assessment will help determine the all-hazards risk profile for the IT Sector, focus resource allocation for protection for the IT Sector to manage its inherent risks, and increase awareness of risks across public and private sectors.

Value Proposition

Coordination of risk management activities by public and private IT Sector security partners should leverage their respective knowledge and expertise while helping focus efforts and resources on ensuring the continued availability of critical IT Sector functions. This process combines individual organizational risk management goals and activities with a perspective and collaborative approach that is nationally significant. Acknowledging and addressing differences between individual and organizational objectives and those of the sector-wide approach offers value by providing individual owners, operators, and security partners with an understanding of the sector perspective and a means to manage IT Sector risk effectively and consistent with national priorities.

Because this is the first effort to assess sector-wide risks, the approach outlined in this section is high level and will evolve and mature through implementation. Future iterations of the IT SSP should reflect a more detailed approach that expands on the concepts in this version.

The IT SCC and IT GCC convened a working group to address the challenge of developing an approach to assess and manage IT Sector risks. The effort considered leading risk management approaches, methodologies, and tools currently employed by sector entities. Given the IT Sector's complexity, global nature, and unique character, the most viable way to proceed is with a qualitative, top-down approach that considers sector security goals and objectives, and then identifies critical IT Sector functions. The resulting sector-wide risk approach focuses on those IT functions with national consequence and is intended to meet and fulfill Sector Goal 1, Prevention and Protection Through Risk Management.

The IT Sector's risk approach fulfills the intent of the NIPP risk management framework by adapting and modifying its activities and concepts to address the unique IT Sector risk environment. The risk assessment approach leverages the baseline criteria outlined in the NIPP, which specify that risk assessment methodologies include an analysis of the human, cyber, and physical elements[19] of infrastructure. In all cases, the human, cyber, and physical elements are assessed in the context of their criticality

[19] Physical elements of infrastructure include tangible property; cyber elements include electronic information and communication systems, and the information contained therein; human elements include critical knowledge of functions, people uniquely susceptible to attack, or the social aspects of infrastructure protection.

to the sector as a whole and the potential for their disruption, damage, or loss to affect the sector. Throughout this section, a common set of terms will be used to describe the IT Sector's risk assessment approach (see text box).[20]

2.1 Background of the IT Sector's Risk Environment

The IT Sector's risk environment is inherently complex and dynamic. A few primary characteristics shape the evolving risk environment: interdependencies between the IT Sector and other critical infrastructure sectors; the highly diverse, virtual, interconnected, and international nature of the IT infrastructure; and the constantly changing threat landscape. The sector has global operations that are interdependent and interconnected with other infrastructures. These operations enhance efficiency and effectiveness and increase the resilience of the sector; however, they daily face numerous multifaceted global threats from natural and manmade events. Many of these threats occur frequently but do not have significant consequences because of individual entities' existing security and response capabilities. However, some of these threats are strategic and could affect critical IT Sector functions. The high degree of interdependency of the IT Sector, its interconnectedness, and non-traceable and unidentifiable actors makes identifying threats, assessing vulnerabilities, and estimating consequences difficult and must be dealt with in a collaborative and creative manner.

Terms

- **Risk:** The expected magnitude of loss resulting from an incident (e.g., terrorist attack, natural disaster) and with the likelihood of such an event occurring and causing that loss.
- **Risk Management:** A planning methodology that outlines the process for setting security goals; identifying assets, systems, networks, and functions; assessing risks; prioritizing and implementing protective programs; measuring performance; and taking corrective action.
- **Threat:** The intention and capability of natural or man-made (intentional or unintentional) events that would be detrimental to the IT Sector.
- **Vulnerability:** A property or characteristic of a function, process, or supporting asset, system, or network that can be exploited for unintended use or can be disrupted by a natural hazard or technological failure.
- **Consequence:** The level, duration, and nature of the loss resulting from the incident.
- **Assurance:** Measure of confidence that the security features, practices, procedures, and architecture of IT Sector products and services accurately mediates and enforces the security policy.

2.1.1 Various Entities' Risk Management Approaches

Risk management approaches used throughout the IT Sector are based on various philosophies, methodologies, and tools. Private sector entities typically base their approaches on business objectives, such as shareholder value, efficacy, and customer service. Regulatory compliance requirements associated with financial reporting integrity and privacy initiatives are increasing awareness across entities within the sector of risk management strategies.

As part of their individual risk management approaches, many IT Sector entities have designated focal points for risk management and/or security. Some have chosen to centralize this function within their organizations while others have chosen to have it distributed across their operations. In addition, IT Sector entities assess various types of risk (e.g., financial, human, supply chain, legal, and compliance) through multiple approaches (e.g., quantitative, qualitative, and modeling and simulation) leveraging both commercial and government off-the-shelf products and customized tools. These entities use a variety of common risk management frameworks to proactively manage steady-state risk (see text box). The list is not all inclusive and not intended to endorse any approach; rather, it is provided as a resource to increase awareness of various methods in use by some sector entities. Appendix 2 provides additional detail on these frameworks.

[20] Although numerous definitions of the terms exist (e.g., from NIST and the International Organization for Standardization (ISO)), the IT SSP bases the terms and definitions on those in the NIPP because the SSP is an annex of that document. The assurance definition is taken from the National Information Assurance Group. Occasionally, the definitions are modified to represent the unique considerations of the sector.

Although outside the scope of this chapter, these individual risk management efforts are designed to support organizational business objectives and, in aggregate, they enhance the security and resilience of the Sector as a whole. A more holistic approach; however, is needed that considers the IT Sector's ability to support the economy and national security.

2.2 Developing an IT Sector Risk Profile

To develop the overall IT Sector risk profile, designated public and private sector security partners will identify critical sector functions collaboratively, analyze threats to those functions, assess vulnerabilities, evaluate consequences, and identify mitigations. A top-down approach will be taken that considers sector goals and objectives to assess whether the current level of risk is acceptable or whether further mitigation is needed in the form of protective programs or other mechanisms designed to reduce risk to an acceptable level. This top-down approach, which focuses on understanding the functions of the infrastructure rather than cataloging physical fixed assets, was determined to be more effective for the highly distributed IT infrastructure. The result is a qualitative assessment of sector-wide risks that public and private IT Sector security partners can use to prioritize additional mitigations and protective measures. Coordination of risk management activities by IT Sector security partners should help focus efforts and resources on ensuring the continued availability of critical IT Sector functions, products, and services and improved resilience of the nationally critical IT infrastructure. This dynamic relationship will be assessed through iterative analysis and is demonstrated in figure 2-1.

Common Risk Management Frameworks

- Control Objectives for Information and Related Technology (COBIT) 3.0/4.0
- Disaster Recovery Institute International (DRII)
- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27000 Series, Information technology—Security techniques—Information security management systems
- ISO/IEC 13335, Information technology—Security techniques—Management of information and communications technology security—Part 1: Concepts and models for information and communications technology security management
- ISO/IEC 17799, 2005 Information technology—Security techniques—Code of practice for information security management
- ISO/IEC 21827, Systems Security Engineering—Capability Maturity Model (SSE-CMM®)
- Information Technology Infrastructure Library (ITIL) Security Management
- NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook
- NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems
- NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems
- Operationally Critical Threat, Asset, and Vulnerability Evaluation℠ (OCTAVE℠)

Figure 2-1: Developing the IT Sector Risk Profile

The sector-wide approach is not designed for use by individual entities and will not arrive at the level of detail of the entities' risk efforts discussed in section 2.1.1. Rather, the approach in the IT SSP examines entities' functions in the context of understanding the risk that could potentially translate to the broader IT infrastructure. To the extent possible, the approach will leverage the entities' existing efforts and best practices across the sector and adapt them to address the IT infrastructure as a whole. This approach will enable individual entities to better understand the impact of their respective risk management strategies on the sector's security posture. By combining individual organizational risk management goals and activities with a perspective and collaborative approach that is nationally significant, the overall security and resilience of the IT Sector is further enhanced.

2.2.1 National IT Sector Risk Management Approach

Successful implementation of the top-down qualitative approach to assessing IT Sector risk depends on collaboration between public and private sector security partners. The risk management approach includes the following steps:

1. Identifying critical functions;
2. Assessing threats, vulnerabilities, consequences, and mitigations:
    a. Analyzing threats;
    b. Assessing vulnerabilities;
    c. Evaluating consequences; and
    d. Identifying mitigations; and
3. Prioritizing risks for the overall sector profile.

Sections 2.3 through 2.5 describe the steps listed above in detail.

2.3 Identifying Critical Functions

The IT infrastructure is an aggregate of primarily virtual and distributed functions supported by various assets, systems, and networks. The distributed nature of the infrastructure inherently provides physical and virtual resilience; however, some functions may have limited supporting cyber, physical, and human elements of the infrastructure that could present risk and potentially increase their vulnerability. Where risk is identified, the Sector will use the assessment process to raise awareness among the entities that rely on the critical functions and propose specific protective capabilities to mitigate risk, where appropriate.

Functions are sets of processes that produce, provide, and maintain products and services. IT Sector functions encompass the full set of processes (e.g., research and development, manufacturing, distribution, upgrades, and maintenance) involved in transforming supply inputs into IT products and services. These functions support the Sector's ability to produce and provide high-assurance products, services, and practices that are resilient to threats and can be rapidly recovered. Assurance is essential to achieving the Sector's vision and is therefore a fundamental aspect of all critical functions. The sub-functions of the critical functions each directly address this aspect and also work in concert to consistently create high-assurance products and services. The IT Sector's functions are not limited by geographic or political boundaries, increasing the need for international collaboration and coordination for not only risk assessment activities but also best practices and protective program design and implementation.

2.3.1 Screening and Assessing Consequences

A top-down approach to assessing functions results in identifying only those functions that meet a minimum consequence threshold. Resources then can be devoted to analyzing nationally consequential functions and their supporting infrastructure.

Criticality of IT Sector functions is assessed based on their potential impact on government or sector missions independent of any specific defined threat scenario (addressed in section 2.4.1). The criticality of a function depends on many factors, such as tolerable magnitude and duration of loss or degradation of that function. The resilience of functions to disruption or degradation increases with the availability of substitutes for the products and services resulting from a given critical function, with the degree of diversity that exists within the functions' processes and with diversity of providers. A disruption or degradation of a function can have a cascading effect if other functions are highly dependent on its outputs. Functions with high dependence and interdependence are of particular concern in this assessment.

IT Sector functions will be screened and prioritized based on HSPD-7 consequence categories and criteria for evaluating nationally significant events. These criteria include the following:

- **Governance Impact:** Effects on Federal, State, and local governments;
- **Economic Security Impact:** Effects on users and the greater economy;
- **Public Health and Safety Impact:** Effects on human health from injuries and loss of life; and
- **Public Confidence Impact:** Effects on the public's morale, caused by the visibility of the impact, number of people affected, and length of time needed to switch to alternative sources.

Table 2-1 identifies critical IT Sector functions[21] and their descriptions based on the consequence criteria described above. These functions are required to maintain or reconstitute the network (e.g., the Internet, local networks, and wide area networks) and its associated services. The list represents IT SCC and IT GCC consensus on critical IT Sector functions that are vital to national and economic security and public health, safety, and confidence.

Table 2-1: Critical IT Sector Functions and Descriptions

IT Sector Function	Description
Provide IT Products and Services	The IT Sector conducts operations and services that provide for the design, development, distribution, and support of IT products (hardware and software) and operational support services that are essential or critical to the assurance of national and economic security and public health, safety, and confidence. These hardware and software products and services are limited to those necessary to maintain or reconstitute the network and its associated services.
Provide Incident Management Capabilities	The IT Sector develops, provides, and operates incident management capabilities for itself and other sectors that are essential or critical to the assurance of national and economic security and public health, safety, and confidence.
Provide Domain Name Resolution Services	The IT Sector provides and operates domain registration services, top-level domain (TLD)/root infrastructures, and resolution services that are essential or critical to the assurance of national and economic security and public health, safety, and confidence.
Provide Identity Management and Associated Trust Support Services	The IT Sector produces and provides technologies, services, and infrastructure to ensure the identity of, authenticate, and authorize entities and ensure confidentiality, integrity, and availability of devices, services, data, and transactions that are essential or critical to the assurance of national and economic security and public health, safety, and confidence.

[21] These are public and private sector consensus critical IT Sector functions for government fiscal year 2007. Annual planning enables the review and update of these functions to reflect changes in the IT Sector environment.

IT Sector Function	Description
Provide Internet-based Content, Information, and Communications Services	The IT Sector produces and provides technologies, services, and infrastructure that deliver key content, information, and communications capabilities that are essential or critical to the assurance of national and economic security and public health, safety, and confidence.
Provide Internet Routing, Access, and Connection Services	The IT Sector (in close collaboration with the Communications Sector) provides and supports Internet backbone infrastructures, points of presence, peering points, local access services, and capabilities that are essential or critical to the assurance of national and economic security and public health, safety and confidence.

2.3.2 Decomposing Critical IT Sector Functions

The IT Sector's approach will decompose the critical IT Sector functions to identify the processes or operations necessary to produce or provide that function. This technique breaks down the functions to a more practical level for analysis, focuses risk assessment efforts on only those processes essential for those functions, and facilitates the understanding of dependencies between processes and their supporting assets, systems, and networks. The IT Sector's approach will decompose its functions by describing the high-level processes generally required to transform inputs into outputs with public and private sector security partners involved in producing or providing the functions.

2.4 Assessing Threats, Vulnerabilities, Consequences, and Mitigations

The IT Sector's approach will evaluate threats to the critical functions, identify associated vulnerabilities, assess consequences, assess the effectiveness of mitigations that are already in place, and identify new or enhanced capabilities needed to manage sector risk effectively. To provide comparable risk assessment results from a sector perspective, consistent measurements will be used for evaluating threats, vulnerabilities, consequences, and mitigations.

2.4.1 Analyzing Threats

IT infrastructure is confronted by various threats; therefore, the threat analysis approach will consider the following spectrum of intentional and unintentional manmade and natural threats:

- Natural threats (e.g., hurricane, fire, floods);
- Cyber threats (e.g., bot networks, data corruption);
- Workforce threats (e.g., pandemic flu, insider threat, industrial espionage, human error);
- Terrorist threats (e.g., chemical and biological attacks); and
- Supply chain threats (e.g., manufacturing plant destruction).

Threats that affect critical IT Sector functions will be assessed for the high-level critical functions themselves and for functions' critical processes. The assessment also will consider policy and operational aspects of each threat and the criteria to determine when a threat is of national concern for IT Sector security partners.

Traditional threat analysis generally identifies an actor and the actor's intentions, motives, and capabilities to compromise a given target. Such approaches typically rely on historical data associated with a particular actor to predict threats. When analyzing threats to the IT Sector, this traditional approach to threat assessment alone is not sufficient in the sector's risk environment because actors are not easily identifiable or traceable, and attacks can go from conception to exploitation within hours. The IT

Sector's approach will complement the traditional threat assessment approach with additional factors based on capabilities and intent independent of known actors to consider emerging nontraditional threats.

The IT Sector's approach will analyze threats that have national significance based on capabilities. The sector defines threat capability as the availability of and/or the ease of use of tools or methods that potentially could be used to damage, disrupt, or destroy critical IT Sector functions. With respect to natural threat, capability is inherent; therefore, natural threats that could have a nationally significant impact will be considered. A capabilities-based approach is applied differently for intentional manmade threats. For intentional manmade threats, the IT Sector is particularly concerned about widely available tools or methods that can be configured easily to exploit critical IT Sector functions. The sector also is vulnerable to unintentional manmade threats because of its high reliance on human interaction and skill sets. The IT Sector's threat approach will include trend analysis of historical data and assessment of capabilities that could destroy, incapacitate, or exploit critical IT Sector functions.

Working together, public and private IT Sector security partners will create strategic and operational threat scenarios based on capability and intent and assess them against critical IT Sector functions. The IT Sector is subject to various threats; consequently, various scenarios will be included in the assessment.

An accurate threat assessment requires collaboration among IT Sector security partners, such as the private sector, the DHS, and other IC partners. Accurately analyzing threats depends on public and private sector security partners generating requirements for collection of threat data and sharing relevant threat information. For example, the DHS through the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)[22] and working in partnership with other IC partners, intends to provide specialized classified and unclassified analytical threat products in the form of threat warnings, incident reports, strategic planning information, target selection matrices, attack-specific threat scenarios, and overall sector-specific threat assessments. Public and private sector security partners are discussing how HITRAC can support the IT Sector threat assessment through future collaboration and requirements development to demonstrate value for customers. Private sector security partners provide a comprehensive understanding of the evolving technological capabilities for emerging threats, their associated consequences, and potential targets. Annually, IT Sector public and private sector security partners will analyze potential threats and determine those of national significance for IT Sector risk assessment.

2.4.2 Assessing Vulnerabilities

To assess vulnerability of the critical functions, the IT Sector's approach will examine associated processes for characteristics that may be exploited by the threat scenarios resulting from the previous step of the risk assessment. Vulnerabilities that, if exploited, could have national consequences are identified and paired with their respective function processes.

Each threat scenario is applied to critical functions' processes and assessed against a set of vulnerability categories (e.g., people, process, and technology). Although these vulnerability categories may intersect or overlap in some cases, the following descriptions will help guide the identification of vulnerabilities:

- **People:** Vulnerabilities associated with critical knowledge of functions, workforce resources susceptible to intentional threats, and the social aspects of infrastructure protection. This category considers factors affecting the workforce such as human resource practices (e.g., personnel security), demographics (e.g., citizenship, qualifications), training and education (e.g., quality and quantity of institutions that teach and train the workforce), and market environment(s) (e.g., compensation and benefits).
- **Processes:** Vulnerabilities associated with the sequence and management of operations or activities. This category includes factors such as manufacturing, logistics, and information flow (e.g., quantity and throughput of distribution channels), con-

[22] HITRAC serves as a national fusion center, bringing together intelligence and infrastructure specialists to integrate, analyze, and share strategic and national-level information regarding the threat of terrorist attack against U.S. CI/KR, including IT and cyber infrastructures. HITRAC capabilities also are discussed in section 4 and appendix 3.

tingency planning and process flexibility (e.g., continuity of operations), and efficiency and effectiveness (e.g., information access globalization).

- **Technologies:** Vulnerabilities associated with integration of technologies within critical functions. This category includes factors such as reliance on hardware and software (e.g., availability, security), and system dependencies and interdependencies.

When identifying vulnerabilities, the sector's approach also will assess the likelihood that the threat scenario will successfully exploit a vulnerability. To ensure a valid assessment of likelihood, the effectiveness of existing mitigations also will be considered. This process will assist the sector in determining where vulnerabilities have been addressed already and where additional mitigations may be appropriate.

2.4.3 Evaluating Consequences

The potential consequences associated with nationally significant events represent the expected range of direct and indirect impacts that could occur should a threat exploit unmitigated vulnerabilities in critical IT Sector functions. The interdependency between the physical and cyber elements of the infrastructure is of particular concern for public and private IT Sector security partners. Conversely, disruption or degradation of cyber elements can have physical consequences as well (e.g., the failure of a control system managing a manufacturing process for IT products). In addition, dependencies and interdependencies between and among critical IT Sector functions will be evaluated and factored into sector risk assessment efforts.

Using HSPD-7 consequence categories and criteria for evaluating nationally significant events, the IT Sector's approach to consequence assessment identifies impacts on national and economic security and public health, safety, and confidence should a critical function be disrupted or degraded. The assessment may consider such questions as, If this function or process is disrupted or degraded:

- Is there a potential for loss of life, injuries, or adverse impact on public health and safety?
- How many users could be severely affected?
- What are the economic impacts, including asset replacement, business interruption, and remediation costs?
- Will Federal, State, and/or local governments be adversely affected? If yes, how much time might elapse before the impact is realized?
- What is the maximum amount of time that the function or process can be disrupted or degraded and still meet the minimal needed functionality in a timely manner?
- Is it possible to switch to alternate source(s)? If yes, how much time is required?

Private sector security partners will collaborate to identify the most appropriate methods for evaluating functions' consequences for their organizations and how best to share the relevant findings with the public sector security partners. Similarly, public sector security partners will collaborate to evaluate functions' consequences from a government perspective. The results of these evaluations then will be combined to understand the overall impacts to the infrastructure.

2.4.4 Identifying Mitigations

Private sector entities implement a vast array of mitigations primarily based on their organizational objectives, whereas public sector interests are focused on assuring the ability of critical IT Sector functions to support the economy and national security. Understanding how existing public and private sector risk mitigations work together to address risks collectively and identifying additional capabilities is an essential component of the IT SSP risk management approach. These capabilities will be considered as part of the process for identifying and implementing new protective programs described in section 3.

The risk assessment approach assesses existing mitigations that reduce threats, vulnerabilities, and consequences, and identifies opportunities for new and enhanced risk mitigation capabilities. These opportunities may exist because of differences between individual organizational objectives and those of the sector-wide approach. Acknowledging and addressing these differences provides value by enabling individual owners, operators, and security partners to understand the sector perspective and manage risk effectively across the sector. Sector-wide risk management activities focus on mitigating, transferring, or accepting risks. At this level, public policy also can be influenced and incentives can be developed for private sector entities to consider a national or sector-wide perspective in their risk management activities.

2.5 Prioritizing for the IT Sector Risk Profile

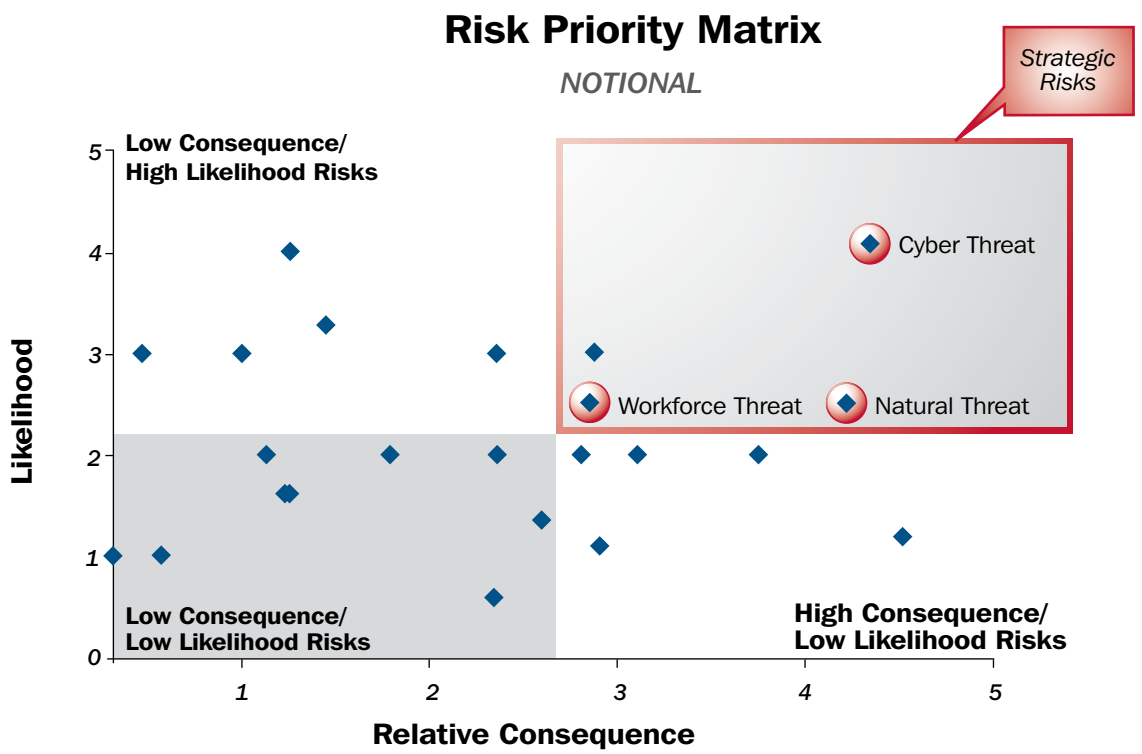
The basic qualitative formula for risk defines risk as a function of threat, vulnerability, and consequence. Threat and vulnerability combined represent the likelihood that a vulnerability could be exploited successfully by a threat.

$$\text{Risk} = f\,(\underbrace{\text{Threat, Vulnerability}}_{\text{Likelihood}}, \text{Consequence})$$

Because limited resources exist to manage the wide range of IT Sector risks, it is important that public and private sector security partners agree on how to best prioritize risks and apply resources to ensure that critical IT Sector functions are protected.

To help determine how to allocate resources, risk priorities will be illustrated on a matrix using consequence and likelihood that a vulnerability will be successfully exploited by a threat. Figure 2-2 demonstrates how threat scenarios may be ranked in relation to one another based on their risk. The IT Sector's approach will focus primarily on strategic risks in the upper right-hand quadrant—those with a high consequence/high likelihood rating.

Figure 2-2: Notional Risk Priority Matrix



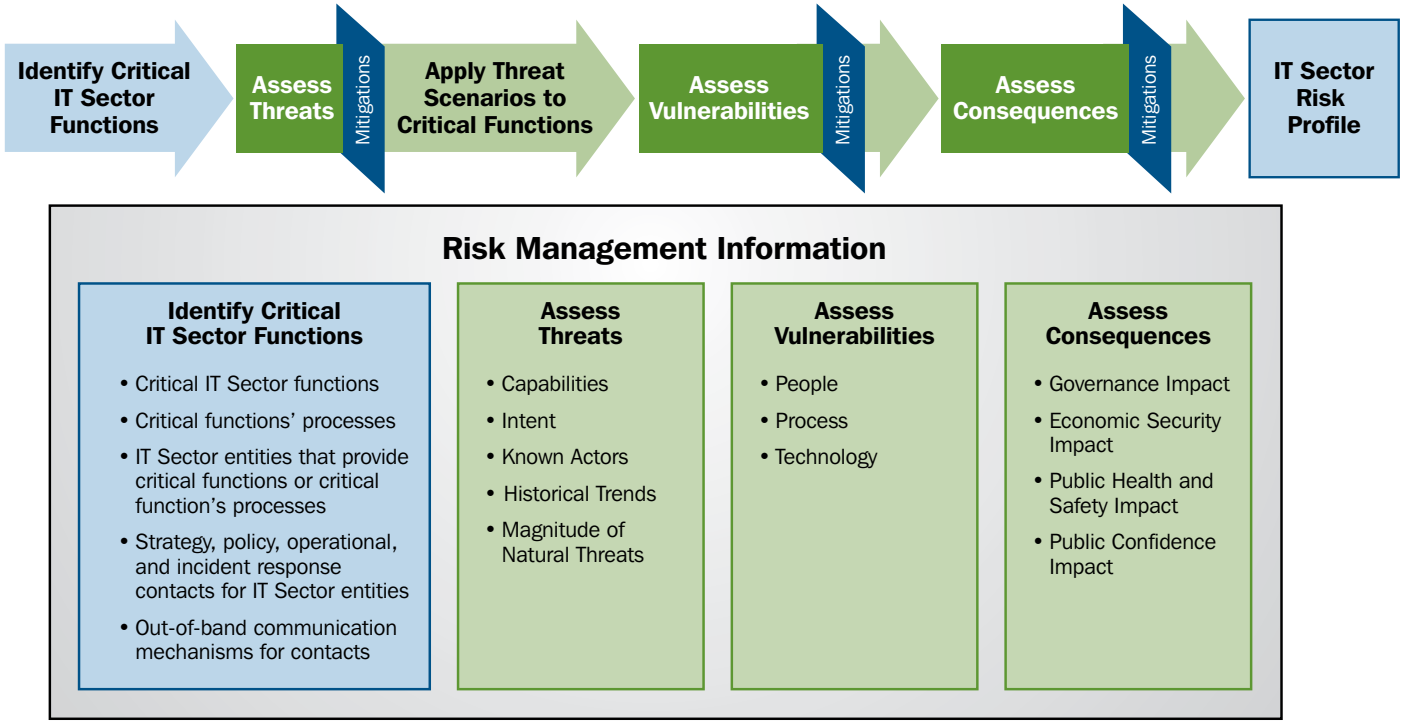
Prioritizing IT Sector risks depends on using consistent measurements for evaluating nationally significant events, comparing results from a sector-wide perspective, and using specific infrastructure information to validate the results. The IT Sector's approach to prioritization will become more defined after completion of actions associated with measurements and thresholds for threats, vulnerabilities, and consequences and described in section 2.7. As such, prioritization will be addressed in greater detail in future versions of the IT SSP.

2.6 Risk Management Information

The implementation of the IT Sector's risk management approach requires commitment from public and private sector security partners. Without active participation of both, the resulting IT Sector risk profile and risk management activities would be inaccurate and ineffective. A collaborative group of public and private sector security partners will implement the national IT Sector risk management approach. Because this group will consist of public and private sector members exchanging operational information, the CIPAC will be used to create a trusted environment for sharing and to afford the protections of the Federal Advisory Committee Act associated with CIPAC. In addition, the sector recommends that a secure Web-based tool be developed to facilitate the sector-wide collaboration necessary to implement the approach and to reach a broader audience of IT Sector entities essential to ensuring the availability and/or reconstitution of the critical functions.

The IT SCC and IT GCC acknowledge that sharing and updating information and assessments of threats, vulnerabilities, consequences, and mitigations are essential to developing a valid IT Sector risk profile. Information needs have been developed collaboratively to ensure that the analysis focuses only on critical IT Sector functions, the specific threats that are being assessed, vulnerabilities that could be exploited by those threats, and the consequences of such events. Figure 2-3 summarizes the composite information derived from a public and private sector partnership needed to support the development of the IT Sector risk profile.

Figure 2-3: Risk Management Information



IT Sector entities' assets supporting the critical functions will be neither requested nor collected as part of this process because the availability, security, and reconstitution of such assets are the responsibility of those entities. The virtual and distributed nature of critical IT Sector functions also makes cataloguing assets impractical and would not yield meaningful results. IT private sector security partners recognize the need to identify and manage information needed to develop the IT Sector risk profile and will accomplish that objective in an arrangement that considers their capabilities, resources, and concerns about the management and protection of such information. The IT SCC and IT GCC will determine the appropriate entity to manage and protect risk management infrastructure information. IT private sector security partners recommend considering use of the IT-ISAC[23] to manage and protect this information because of the proven and trusted relationship, reinforced by contractual obligations, that exists between the IT-ISAC and private sector entities. The actions described in section 2.7 provide additional detail about the roles of public and private sector security partners in identifying and providing this information.

2.7 Actions

The following bulleted list includes near term and long term actions to be completed to implement this section of the SSP.

2.7.1 Near Term (~1 year)

Actions to Develop the IT Sector Risk Profile

- Develop an implementation plan for the 2007 IT Sector Risk Profile. *(NCSD with GCC and SCC input)*
- Identify resources needed to implement the 2007 IT Sector Risk Profile. *(NCSD with GCC and SCC input)*
- Select the appropriate entity to manage and protect IT Sector risk management information. *(SCC, IT-ISAC, and GCC)*
- Decompose the sector's critical functions and/or sub-functions. *(SCC, IT-ISAC, and GCC)*
- Develop initial draft measurements and thresholds for evaluating consequences, vulnerabilities, and threats consistently to enable comparable risk assessment results. *(SCC and IT-ISAC with GCC input)*
- Initiate the identification of the sector's nationally consequential threats, and conduct analysis of them against the critical IT Sector functions. *(GCC, IT-ISAC, HITRAC, and IC)*
- Initiate the identification and assessment of vulnerabilities and consequences for critical IT Sector functions. *(IT-ISAC with GCC input)*
- Initiate the identification and assessment of mitigations that address threat, vulnerability, and/or consequences. *(IT-ISAC and GCC)*
- Collaborate with the Communications Sector regarding the identification and risk assessment of the Internet infrastructure, including specifically physical and cyber threat assessments for the Internet. *(SCC, IT-ISAC, and GCC)*

Other Actions:

- Continue to encourage participation in the IT SCC and IT GCC. *(SCC, IT-ISAC, and GCC)*
- Encourage IT Sector entities to consider adopting individual risk management approach(es) appropriate for their unique operating environments. *(SCC and IT-ISAC)*
- Collaborate and coordinate with the other CI/KR sectors to address threats outside the IT Sector's control. *(SCC, IT-ISAC, and GCC)*

[23] Section 4, Information Sharing, provides additional detail about the IT-ISAC.

2.7.2 Long Term (1-3 years)

- Review (annually) critical IT Sector functions to determine if technological and environmental changes have occurred that alter the set of functions or their descriptions. *(SCC and GCC)*
- Identify (annually) threats, vulnerabilities, consequences, and mitigations that are of national significance to the sector. *(SCC, IT-ISAC, GCC, HITRAC, and IC)*
- Define and refine the IT Sector risk profile over time as the approach described in this section is implemented and repeated. (GCC, SCC, HITRAC, and IC)
- Improve cross-sector coordination. (SCC, IT-ISAC, and GCC)

3. Develop and Implement Protective Programs

Protective programs include measures or activities that are undertaken by various security partners to prepare for, prevent, protect against, respond to, and recover from incidents that have the potential to affect critical IT Sector functions. Programs are sponsored and/or led by public or private sector security partners, or they represent a partnership between the public and private sectors. Protective programs facilitate progress toward achieving the sector's goals. Protective programs are characterized by actions to:

- Define needs and objectives to ensure efforts are comprehensive and sustainable;
- Respond to the needs of various security partners;
- Apply appropriate resources in a cost-effective and efficient manner (e.g., people and funding); and
- Ensure accountability for performance.

Value Proposition

The private sector's experience protecting, restoring, and reconstituting the IT infrastructure is a critical resource to the government in identifying future protective program needs, determining the overall effectiveness of protective programs to meet IT Sector goals, and implementing and/or participating in protective programs. The government provides resources and coordination for national-level programs. Whether protective programs are voluntary industry initiatives or national-level efforts sponsored by the Federal Government, the identification, development, and effective implementation of such programs facilitate risk management, situational awareness, and response, recovery, and reconstitution goals of the IT Sector.

This section presents an overview of the IT Sector's strategy and describes the process for developing protective programs that mitigate risk.

3.1 Current IT Sector Protective Programs

Table 3-1 describes protective program capabilities that support IT Sector goals. Additional information regarding existing protective programs, including a brief description of each, is provided in appendix 5. The list of protective programs in appendix 5 is not exhaustive. Rather, the programs are initial examples of sector protective programs (primarily federally sponsored) that address the sector's goals. Several protective programs encompass protective measures and activities that apply not only to the IT Sector but also to many other critical infrastructure sectors.

Table 3-1: Protective Program Capabilities that Support IT Sector Goals

Goal	Outcome and Capability	Services Provided by Protective Programs
Prevention and Protection Through Risk Management	Vulnerability Reduction	A means to identify and obtain timely information on sector vulnerabilities; access to remediation and mitigation actions and best practices.
	Threat Analysis	An understanding of the threats facing the IT Sector and the Nation today and in the future.
	Modeling and Simulation	Capabilities to analyze and understand critical infrastructure interdependencies.
	High-Assurance Products and Services	Products and services with built-in security.
	Security Best Practices	Mechanism for identifying and sharing IT security best practices and protective measures.
Situational Awareness	Tactical Indications, Analysis and Warning	Information about incidents and other events as they are detected and unfold to raise awareness and understanding of the current operating environment.
	Information Sharing and Communications	A means for accessing and sharing information that enables decision makers to understand the current operating environment, form an opinion about the current state of security, and take action to respond to the events around them.
Response, Recovery, and Reconstitution	National Emergency Communications	Mechanisms to ensure that public and private sector security partners can communicate with one another during incidents.
	Incident Management and Incident Response Coordination	Capabilities to coordinate efforts to detect, contain, eradicate, and recover from incidents. Furthermore, analysis of lessons learned throughout each incident management life cycle phase enhances security partners' preparedness and prevention capabilities.
	Investigation and Attribution	Methods for attributing incidents to a person or persons with the ultimate goal of apprehending and prosecuting the suspected responsible parties.
	Contingency Planning/National-Level Planning	Actions that facilitate the exercise of plans, processes, and procedures to ensure individuals, organizations, the sector, and the Nation can respond and recover from incidents. Formal resource planning and allocation helps security partners identify needs for and uses of available mechanisms for coordination of materials and expertise to facilitate recovery.

Individual organizations also voluntarily implement protective initiatives and programs designed to enhance their physical, cyber, and human security. Taken together, these individual actions and measures enhance the overall security of the IT Sector. Examples of these actions include physical vulnerability mitigation measures (e.g., physical access control and surveillance), human vulnerability mitigation measures (e.g., employee screening and security training and awareness), cyber security measures (e.g., encryption), and business continuity planning. Such individual protective actions are outside the scope of this document.

3.2 Identification and Implementation of New Protective Programs

The following describes a process to determine the IT Sector's types of protective actions necessary to address priorities identified through the sector's risk management approach. This process will be used where individual entities cannot provide the mitigation, no viable private sector solution exists for meeting the need, or high transaction costs, legal barriers, or other impediments would cause significant coordination or implementation challenges.

3.2.1 Establish a Protective Program Working Group

An IT Sector Protective Program Working Group should be established to accomplish the following:

- Determine whether existing programs adequately promote the security of critical IT Sector functions;
- Identify any desired capabilities needed to address risk;
- Frame future protective program needs; and
- Make recommendations to the IT SCC and GCC for specific protective programs.

An effective Protective Program Working Group should include public and private sector representatives from entities such as the NCSD, IT SCC, IT GCC, and other security partners (e.g., representatives from other CI/KR sectors).

3.2.2 Determine Needs and Capabilities

The Protective Program Working Group will identify areas where protective measures are most needed to achieve the sector's goals. During the initial SSP development process, IT SCC and IT GCC members identified the following examples of capabilities that may be further considered in order to enhance the security of the IT Sector:

- **Robust Coordinated Response Capabilities.** The capability to respond to and recover from a nationally significant event is critical to promoting the resilience of the IT Sector and other CI/KR sectors. An all-hazards operational response and recovery capability is needed to bring public and private sector security partners together to coordinate activities. Emergency communications, collaboration, and analytical tools could enhance effective response; this may include bolstering existing public and private sector resources and capabilities.
- **Reconstitution of Data.** Data reconstitution tools and techniques are needed to ensure the integrity and availability of data. Development of a protective program should be linked closely to R&D activities designed to develop and pilot capabilities that enable key public and private sector systems to reconstitute rapidly data that could be corrupted, either intentionally or unintentionally.
- **Reconstitution of Communications Services and Networks.** A protective program initiative may be developed to assist with implementation of Federal Government authorities under Section 706 of the Communications Act applicable to key Internet functions. This program should also include developing the plans, programs, and mechanisms for identifying and refining requirements and developing reconstitution capabilities.

- **Out-of-Band Data Delivery Capability.** A protective program initiative is needed to provide mechanisms for delivering patches and other software to critical users if key Internet/network functions are not available. Such programs could include procuring space on satellites or unused television spectrum for moving software (e.g., critical patches or software) to key sites during a crisis or network congestion/failure.
- **Grants.** DHS should consider leveraging the existing grants process to more explicitly provide cyber security requirements for key State government operations that emphasize State activities, align them with Federal activities and the priorities described in the National Strategy to Secure Cyberspace, and enhance the States' operational cyber security.

The SSP development process also revealed that capabilities may be needed to facilitate the (1) development and demonstration of high-assurance products and services, (2) development and implementation of secure protocols, and (3) implementation of routine exercises and assessment of cyber security.

IT SCC and IT GCC members anticipate that additional needs and capabilities will be identified as the IT Sector's risk assessment approach is implemented. IT SCC and IT GCC efforts will provide the foundation for development of the IT Sector Annual Report, which will further define IT Sector protective program needs and priorities.

3.2.3 Identify Protective Actions

The Protective Program Working Group will identify protective activities to fulfill identified needs. The working group will consider the desired capabilities or outcomes that the program must achieve and the actions needed to provide those capabilities and outcomes. This effort will be linked closely with R&D efforts to ensure that activities for addressing desired capabilities are being developed and will be in the pipeline for implementation.

3.2.4 Develop an Implementation Plan

An initial implementation plan will be developed by the Protective Program Working Group for identified needs. The plan will include recommendations regarding the party or parties responsible for implementing the program, schedule, resources (e.g., facilities, budget, processes, and procedures), coordination with other programs, next steps, potential obstacles to success, and other considerations for successful initiation and maintenance of the program. Implementation of enhancements to existing programs or development of new protective programs may be filled by owners and operators, either voluntarily or based on various forms of incentives, or by cross-sector or national efforts undertaken by the Federal Government.

3.3 Protective Program Performance

Ongoing performance measurement will ensure that program performance aligns with intended IT Sector goals and will identify opportunities for continuous improvement. Federal departments and agencies, State and local governments, and organizations and associations that manage and oversee protective programs typically measure the performance of their programs just as owners and operators measure the performance of mitigation actions they use to enhance security.

Taking this into consideration, the IT SCC and IT GCC will meet annually to review overall progress toward IT Sector goals. During this annual meeting, IT SCC and IT GCC representatives will consider available information that reflects the progress of individual programs (e.g., Performance Assessment Rating Tool measures, program reviews), general views regarding needed capabilities, and the overall effectiveness of each protective program area. Review of individual programs will be left to those responsible for the program's implementation and maintenance. The IT Sector's approach to protective program performance and the review of overall progress follows the overall approach for tracking progress of IT SSP implementation as described in section 7.

3.4 Actions

The following bulleted list includes near term and long term actions to be completed to implement this section of the SSP.

3.4.1 Near Term (~1 year)

- Establish the joint IT SCC and IT GCC Protective Program Working Group to review existing protective programs, identify private sector programs, and refine and consolidate the list of current programs. *(NCSD, SCC, and GCC)*
- Hold annual meeting on protective programs before developing the IT Sector CI/KR Protection Annual Report. *(NCSD, SCC, and GCC)*

3.4.2 Long Term (1-3 years)

- Raise awareness of elected and appointed officials in all branches of State government of the IT Sector's role in CI/KR protection. *(NCSD with SCC, GCC, and NASCIO input)*
- Report on protective program successes and lessons learned in the IT Sector CI/KR Protection Annual Report. *(NCSD with SCC and GCC input)*
- Conduct joint discussions with the Communications Sector on protective program effectiveness and requirements for new protective programs to avoid duplication of efforts. *(NCSD, SCC, GCC, NCS, Communications SCC, and Communications GCC)*
- Manage protective programs sponsored by the Federal Government in close partnership with the private sector. *(NCSD, GCC, and other Federal departments and agencies)*

4. Information Sharing

Information sharing is a key element to fulfilling IT Sector goals and implementing the NIPP framework. Information sharing enables owners and operators, decision makers, managers, and others to detect, deter, and prevent attacks and incidents, identify trends, assess risks, provide warnings to help mitigate impacts, and coordinate response activities. Elements of information sharing include the following:

- Production of the information;
- Timely distribution of the information to specific, trusted partners and broader audiences; and
- Analysis and use of the information.

This section of the SSP describes the types of information that are important to IT Sector security partners and how that information is to be shared within the sector. This section also describes the following:

- Current IT Sector information sharing initiatives;
- Key focal points for policy and operational information sharing;
- Proposed process and procedural enhancements;
- Ways to provide greater access to information; and
- Near term (~1 year) and long term (1-3 years) actions to improve information sharing.

Value Proposition

Participation in the exchange of information among and between the public and private sectors provides a coordinated mechanism that will support the management of incidents, ultimately improving business continuity, continuity of operations, and resilience of IT Sector critical functions. Sharing timely and actionable information with security partners better enables them to prevent, protect, respond to, or recover from cyber or physical events, technological emergencies, or presidentially declared disasters that threaten, disrupt, or cripple IT Sector infrastructure.

The ISAC Council Framework for Operational Information/Intelligence Sharing (Version 1.0, October 2006) provided a foundation for considering concepts and topics included in this section. The Council's framework provides a high-level set of components, which are part of an effective and manageable CI/KR protection information sharing infrastructure.[24]

4.1 Types of Information

To be useful, information must be timely, relevant, actionable, and labeled so that recipients know the type of information and its sensitivity. The following descriptions of the categories of information that are produced, shared, and used by the IT Sector are consistent with information categories identified by the ISAC Council framework.

[24] Additional information on the ISAC Council may be found at www.isaccouncil.org.

- **Analytical Product.** An analytical product contains the documented conclusions of public and private sector subject matter experts derived by applying threat information against known or perceived vulnerabilities to determine the likelihood of occurrence and the potential consequences. Analytical products include the following types of analysis:
  - ***Tactical Analysis*** examines factors associated with incidents under investigation or identified vulnerabilities to generate indications and warnings.
  - ***Strategic Analysis*** looks beyond individual incidents to consider broader sets of incidents or implications that may indicate threats of potential national importance. For example, strategic analysis may identify long-term threat and vulnerability trends that could provide advanced warnings of increasing risks, such as emerging attack methods. Strategic analysis gives decision makers information they can use to anticipate and prepare for attacks, thereby diminishing the potential damage. Strategic analysis also provides a foundation to identify patterns that can support indications and warnings.
- **Data.** Data include electronic, voice, or printed information routinely provided to trusted members for specified CI/KR protection purposes. Data products include the following types:
  - ***Key Resources Data*** is a list of assets and their locations (i.e., in the context of CI/KR protection, the building blocks of a critical infrastructure).
  - ***Risk Data*** pertain to information regarding the potential consequences to assets, functions, or services at risk, should the incident under study actually occur.
  - ***Vulnerability Data*** can be used to assess the degree to which given assets, functions, or services are vulnerable to the threat posed by the potential incident under study.
- **Incident Report.** An incident report should include details regarding the incident that has occurred, where it occurred, and when it occurred. The impact of the event will be reported as situational awareness.
- **Mitigation Actions.** Mitigation actions are operational practices that individual entities employ to enhance the security of their organizations. Examples include application of enterprise solutions to patch management, change management, configuration management, identity management, or procurement of secure systems. Entities may share information with one another or with other sectors regarding effective enterprise security practices.
- **Needs Requirement.** A needs requirement is any formal request for information (RFI) related to a threat, vulnerability, or incident.
- **Open Source Information.** Open source information is information available for non-restricted distribution.
- **Situational Awareness.** Situational awareness is an assessment of how an event affected specified assets and infrastructure, including consequential impacts on other infrastructures, missions, and functions. Situational awareness information includes the following:
  - ***Advisories*** are formal, narrative information bulletins intended to advise the recipient of certain facts, such as new threat information, the occurrence of an incident, or other information.
  - ***Alerts*** are indicators of a change in state. An alert is an advisory of an urgent nature. Alerts can be triggered for numerous reasons, including suspicious activity, aberrations or abnormalities detected during operations, or other information requiring increased awareness or attention from the sector. Although an advisory notifies and informs, an alert is a call to action.
  - ***Threat Warning*** provides information about an existing or developing threat that may lead to an incident. A warning is specific and actionable rather than merely stating a general concern about a potential event. A warning pertains to events that are imminent.

In addition to these information-sharing categories, information often has varying degrees of importance and uses. For example, shared information may be time sensitive, or it may be provided for long-term strategic use. Likewise, information may be of varying degrees of sensitivity, such as classified, unclassified, sensitive, proprietary, or open source. In addition, information often is disseminated in a tiered or phased approach based on disclosure constraints related to the sensitivity of the information.

4.2 Information Originators and Users

Public and private IT Sector security partners focus on building and maintaining trusted relationships to fulfill the IT Sector's goals based on the simple premise that, for information to be useful, it must be shared with the right people at the right time. This section focuses on sharing information between and among the government and those individuals who own, operate, and administer the IT infrastructure.

Information sharing often is done voluntarily. Private sector entities typically are not required or mandated to share information. In fact, private sector entities may even face Federal or State government limits on disclosure of sensitive information, and contractual obligations may restrict how and when information is disclosed. Information sharing within the public sector often is complicated by authorities and mandates governing information-sharing activities. For example, government may face difficulty sharing information because of its sensitivity (e.g., Privacy Act limitation on disclosure of personally identifiable information). Conversely, the government may be required to disclose information under the Freedom of Information Act (FOIA) or equivalent State disclosure laws.

A two-way flow exists between information originators and users. Information users are also information providers and vice versa. Each provides value to the information-sharing cycle. For example, entities that provide information determine how, when, and with whom to share the information and any restrictions that apply. Those who receive it determine how they will use it. Figure 4-1 describes the role of information originators and users.

Figure 4-1: Information Flows

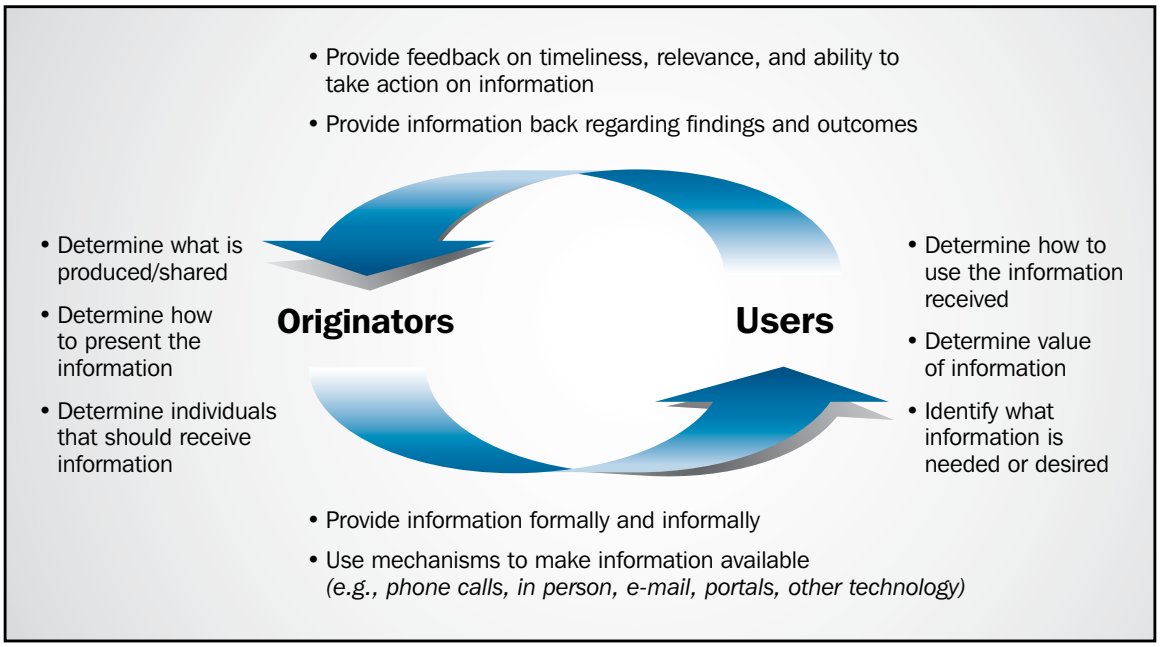
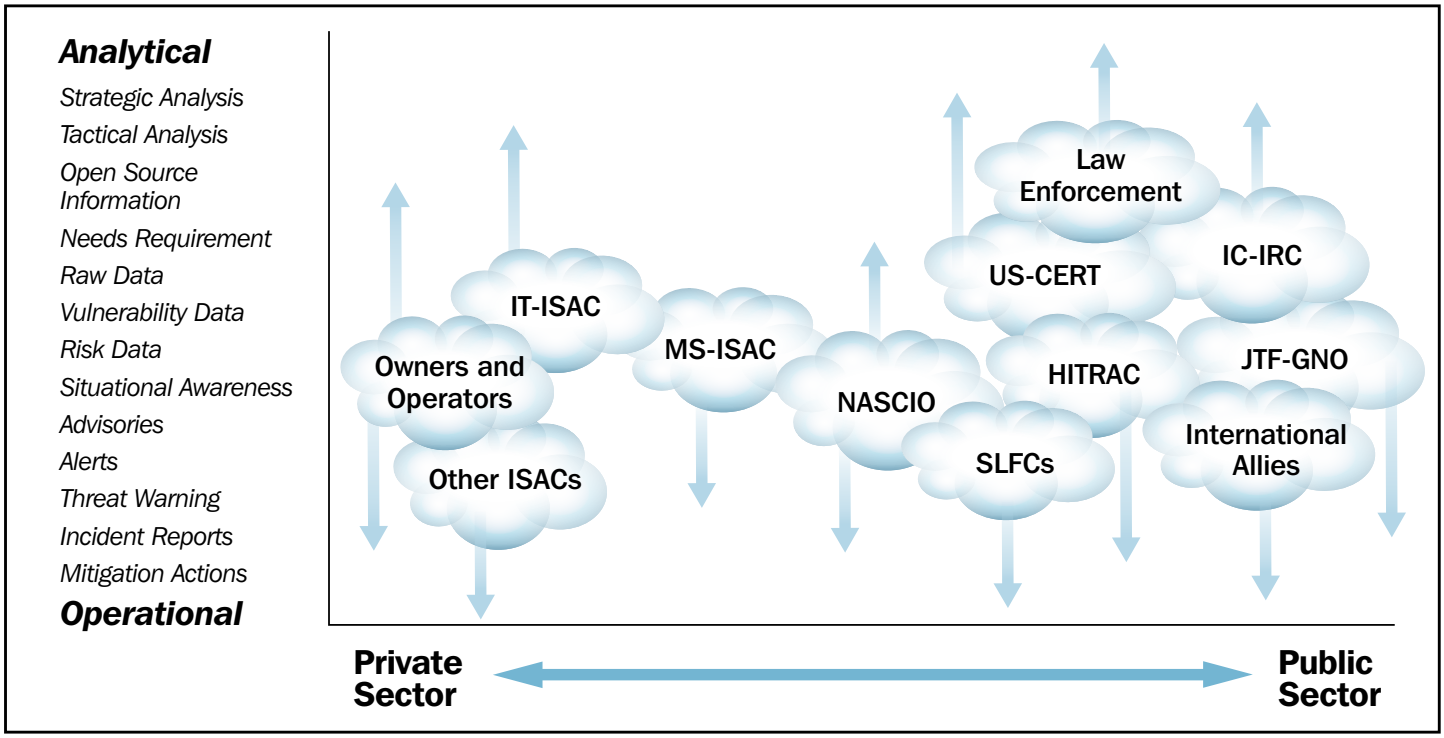


Table 4-1 provides a template for describing entities engaged in the information sharing cycle. It is a notional representation of a much larger and dynamic community of information sharing partners. Figure 4-2 illustrates the relationship between originators and users of the various types of information. The list of entities presented in Table 4-1 and Figure 4-2 are not all inclusive. Similarly, figure 4-2 only begins to describe the extent to which information is shared with others. Much additional work is needed to characterize and map who has the information, how it is shared, and with whom it should be shared. A near-term action to accomplish this effort is described in section 4.4.

Table 4-1: Types of Information Produced by Security Partners (Notional Template)

Information Originator	Category of Information											
	Analytical Products	Data: Raw Asset	Data: Risk	Data: Vulnerability	Incident Reports	Mitigation Actions	Needs Requirements	Open Source Information	Situational Awareness (SA)	SA: Advisories	SA: Alerts	SA: Threat Warning
IT-ISAC	X	X		X	X		X	X	X	X	X	
US-CERT	X	X	X	X	X	X	X	X	X	X	X	X
MS-ISAC	X	X		X	X		X	X	X	X	X	
Other ISACs	X	X		X	X		X	X	X	X	X	
NASCIO	X		X	X		X	X					
HITRAC	X								X			X
IC-IRC	X	X		X					X		X	X
JTF-GNO	X	X	X	X	X	X	X	X	X	X	X	X
NOC									X			
NICC	X				X		X		X		X	
Federal Law Enforcement Community	X				X	X		X	X	X	X	X
SLFCs	X						X	X	X			X
International –Allies	X	X	X	X	X	X	X	X	X	X	X	X

Figure 4-2: Notional Relationship Among Security Partners and Types of Information



4.3 An Enhanced IT Sector Information Sharing Framework

Implementing the IT Sector's vision for information sharing may require changes in policy, culture, organization, and technology to create the conditions that facilitate two-way, decentralized, coordinated, and trusted information sharing. Together, public and private sector entities and individuals can build an effective information-sharing environment that accomplishes the following:

- Facilitates the flow of information between and among public and private sector security partners in a timely, consistent, and predictable manner within a trusted environment, where information is received, disseminated, analyzed, and protected appropriately;
- Fosters a "need to share" culture, where incentives for sharing, especially for private sector entities, are realized clearly through value-added products and information;
- Identifies single points for coordinating information and assigns accountability, ensuring that information is being passed to the appropriate individuals;
- Establishes clear roles and responsibilities to help all security partners know how they fit into the information sharing landscape;
- Focuses on organizational levels, ensuring that established communication lines remain intact even when an individual leaves;
- Articulates incident reporting thresholds to define what constitutes an "incident" and ensures that a common baseline of corresponding actions exist for each level of severity;

- Creates uniform processes for protecting and disseminating information to ensure data are handled and distributed consistently across organizations and security partners to prevent unwanted disclosure; and
- Employs interoperable systems to enable users to communicate and exchange data efficiently across jurisdictional and organizational boundaries.

4.3.1 Information Sharing Focal Points

The IT Sector's vision related to focal points for information sharing is presented below:

- Institute an information sharing environment that ensures security partners can receive and disseminate information effectively and efficiently;
- Ensure that channels for building trusted relationships at the organizational level are institutionalized and considered routine practice;
- Obtain buy-in at the organizational level, ensuring that communications among partners are maintained regardless of personnel changes that take place within a company or government department or agency; and
- Ensure that security partners understand their respective roles, responsibilities, objectives, and incentives for sharing.

Achieving this vision requires designating organizations as focal points for gathering, analyzing, and disseminating information in a coordinated, reliable, and efficient manner. Defining these primary focal points and clarifying roles and responsibilities assigns accountability for accomplishing the IT Sector's vision for sharing information with the right people at the right time.

- **Current Initiatives:** The IT Sector has conduits for sharing information about policy issues and for sharing operational-level information. The primary conduits for policy issues are the IT SCC and IT GCC. The primary conduits for operational-level information exchange include the IT-ISAC for the private sector; the United States Computer Emergency Readiness Team (US-CERT); and the MS-ISAC for Federal, State, local, and international governments. Identification of key focal points for IT Sector information sharing enables the sector to maintain the flow of information and communication during contingencies.
- **Policy Mechanisms:** Consistent with the NIPP Base Plan, the IT SCC and IT GCC serve as the primary bodies for exchanging information on sector-wide policy issues pertinent to the IT Sector. As the strategic leadership for the IT Sector, representatives from both organizations work in close coordination to plan, develop, and coordinate sector-wide programs and initiatives, strategies, and policies. Other security partners play a role in policy-related information exchange and provide feeds into and use information generated by these two bodies. Through information exchange and collaboration, the IT SCC and IT GCC ensure that sector policies are coordinated and consistent with other national-level initiatives, other infrastructure sectors, SSAs, and other relevant parties, such as the PCIS and the Federal Senior Leadership Council, as needed.
- **Operational Mechanisms:** Consistent with the NIPP partnership model and fully endorsed by the IT SCC, the IT-ISAC is the IT Sector's focal point for coordinating the sharing and analysis of private sector information (operational and strategic) between and among members as well with other public and private security partners, including Federal, State, and local governments, international entities, and academic institutions. The IT-ISAC serves as a central repository for security-related information about threats, vulnerabilities, and best practices related to physical and cyber events, and is responsible for the receipt and dissemination of this information to ISAC members. The IT-ISAC also communicates with US-CERT and other sector-specific ISACs. Together, these capabilities offer members a current and coherent picture of the IT Sector's security.

  US-CERT is a partnership between the DHS and the public and private sectors designed to facilitate protection of cyber infrastructure and to coordinate the prevention of and response to cyber attacks across the Nation. US-CERT is a 24/7 single point of contact (POC) for cyber analysis, warning, information sharing, and incident response and recovery for security partners, including the IT Sector. US-CERT interacts with Federal departments and agencies, including the IC (via the IC-IRC), the

private sector, academic and research community, State and local governments, the international community, and others to disseminate reasoned and actionable cyber security information to the public.

For State governments, the MS-ISAC serves as a focal point for information sharing with and among State and local governments. The MS-ISAC is a voluntary and collaborative organization with participation from all 50 States and the District of Columbia. It provides a common mechanism for raising the level of cyber security readiness and response in each State and with local governments. The MS-ISAC provides a central resource for gathering information on cyber threats to critical infrastructure from the States and providing two-way sharing of information. In addition, the DHS officially has recognized the MS-ISAC as the national center for the States to coordinate cyber readiness and response. The MS-ISAC and US-CERT exchange information regularly to facilitate national coordination of cyber security detection, prevention, and response activities.

The establishment of SLFCs across the Nation also provides a mechanism for the two-way flow of timely, accurate, actionable, all-hazard information between State and local governments and intelligence and law enforcement communities. SLFCs are multidisciplinary information-sharing hubs that bring together Federal, State, and local governments, law enforcement, and the private sector. During a regional or national event, SLFCs are intended to be central mechanisms for coordinating intelligence, resources, and situational awareness across the various levels of governments and with the private sector. Efforts to establish and operate SLFCs continue to evolve. Governance, staffing, funding, training, tools, processes, and technology are being identified, instituted, exercised, and maintained. As the capabilities and needs of the SLFCs mature, the IT SCC and IT GCC will define their relationship with the SLFCs.

4.3.2 Policies and Procedures for Sharing and Reporting Incidents

The IT Sector's vision for sharing and reporting incidents is provided below:

- Collect, disseminate, and share information along horizontal and vertical paths of an organization and among organizations;
- Communicate in a regular and predictable manner so that information is passed to all appropriate security partners and entities are not inadvertently omitted;
- Establish formal policies or procedures to prescribe the flow of information between and among public and private IT Sector security partners at all levels; and
- Develop formal triggers or incident-reporting thresholds to provide consistent guidance to owners and operators for determining when to elevate an event to a higher level or report it to the government.

Fulfilling this vision is critical to institutionalizing the timely and routine dissemination of information that fosters a culture of a "need to share" and minimizes duplication of effort.

Current Initiatives: The IT-ISAC has developed a template for organizations to use for sharing information with one another through the key focal points for IT Sector operational information sharing (i.e., IT-ISAC, US-CERT, and MS-ISAC). The structure for reporting information includes identifying the sender, target audience, use and/or type of information (e.g., general information, general action, analytical product, RFI, alert), sensitivity of the information, rules for disclosure, and timeliness of the information. Use of this template is supported by the IT-ISAC, the ISAC Council, and elements of DHS, including US-CERT. Broad acceptance across and use by private IT Sector security partners is desired.

4.3.3 Procedures for Protecting and Disseminating Sensitive Proprietary Industry Information

The IT Sector's vision regarding protecting and disseminating industry information is provided below:

- Work within an information-sharing environment that includes rules, policies, and procedures for protecting data to ensure that shared data are protected adequately and consistently across public and private sector organizations;

- Protect sensitive proprietary data from improper disclosure so that business integrity and public confidence are maintained and trust between and among public and private sector security partners is fostered; and
- Provide the appropriate operational and technical means to protect and secure data to ensure the integrity, availability, and confidentiality of the information.

Current Initiatives: The IT-ISAC and other information sharing organizations have implemented strict submission and classification guidance to protect sensitive proprietary data from unwanted disclosure. Membership in the IT-ISAC is dependent on adherence to these rules, which are enforced through contractual agreements. Members can submit information anonymously or with attributable, identifying information depending on their preferences or the sensitivity of the information. They also may label submissions designating who can view the information (e.g., the public, IT-ISAC membership, or only the ISAC for trending and analysis purposes). Submitted information is protected appropriately according to labeling requirements. Memorandums of understanding (MOUs) with partners and a consistent labeling framework help ensure that rules and procedures for sharing information are followed. For example, MOUs with other sector ISACs facilitate the exchange of threat and vulnerability data across sectors. This information is vital to assessing IT Sector risk and also helps other infrastructure sectors understand risks posed by vulnerabilities in the IT Sector.

Protected Critical Infrastructure Information (PCII) Program: To protect information that is voluntarily shared with the Federal Government, Congress passed the Critical Infrastructure Information Act of 2002 (CII Act), Subtitle B, of the Homeland Security Act of 2002, Public Law 107-296. The CII Act's purpose is to encourage the private sector to voluntarily submit CII, which often contains proprietary and confidential information, to the DHS by protecting CII from disclosure under FOIA and State and local government open records laws, and from use in civil litigation. The CII Act authorizes the DHS to receive voluntarily submitted information that qualifies for protection and to give it special protection as specified by the CII Act. In accordance with the act, the DHS established the PCII Program to encourage infrastructure owners and operators to share sensitive information voluntarily.

The PCII Program Office receives, evaluates, stores, and shares voluntarily submitted information that qualifies for protection under the legislation. Submissions under the program may be used for various homeland security purposes, including analyzing sector risk and vulnerabilities, securing and protecting systems, and informing response and recovery efforts. PCII is shared with Federal, State, and local governments that are certified to handle PCII and provides a feed into tactical and strategic analysis, vulnerability assessments, alerts, and other products that are shared with various audiences. Federal departments and agencies and State and local governments are among those that have been certified to handle PCII and are using the program to facilitate the sharing of information. The PCII Program also provides a single submission entity to reduce duplicative requests for information. Despite the establishment of the PCII Program, many private infrastructure owners and operators remain hesitant to share information and are unsure about the department's ability to protect their information. In addition, the benefits to the private sector of sharing sensitive information have not been articulated clearly, although the associated risks are clear.

4.3.4 Access to Classified and Sensitive But Unclassified (SBU) Government Information

The IT Sector's vision for sharing classified and SBU government information is provided below:

- Ensure that all key partners, including State and local government officials and private industry personnel, have the requisite clearances for obtaining access to pertinent threat data and analyses provided by the IC;
- Promote uniform policies and procedures governing the designation, handling, and distribution of sensitive data such as law enforcement sensitive (LES), for official use only (FOUO), and SBU data; and
- To foster trust by ensuring uniformity and consistency in the level of protection afforded and rules or circumstances for further dissemination, which both help to minimize the risk of compromise and improper disclosure.

Current Initiatives: Security clearances and classifying data enable the Federal Government to protect and restrict access to sensitive or classified information to those with requisite background investigations and a demonstrated need to know. Strict handling and dissemination rules for classified data ensure appropriate and consistent protection and dissemination of that data. Federal departments and agencies have been working with the IT SCC and State and local government officials to grant security clearances to private sector and State and local government officials. The Federal Government, in particular the IC, has been working to develop regular processes for sanitization and production of classified information in a way that allows it to be shared, even if it comes from sensitive methods and sources (e.g., tear-line reports). For example, HITRAC is developing and providing periodic classified threat briefings and reports to appropriately cleared IT Sector security partners and other infrastructure sectors.

4.3.5 Mechanisms for Communicating and Disseminating Information

The IT Sector's vision for information communication and dissemination mechanisms is provided below:

- Ensure automated communication tools can send broadcast messages or alerts to a defined community of users, provide forums for the exchange of information on vulnerabilities, and raise awareness of security issues; and
- Have access to and use of tools for information exchange—whether voice, data, and network based—that are secure, robust, survivable, and interoperable.

Current Initiatives: Technology is a key enabler for effective information sharing. It provides security partners the means to share and exchange various types of data in real time and across jurisdictional and organizational boundaries, enabling key partners to work from a common understanding of the situation. IT Sector security partners use various communications tools to exchange information with each other and with other sectors. These tools facilitate the exchange of information between individuals and larger communities or audiences as needed.

Regular meetings and conference calls also provide a mechanism for exchanging various types of information. The IT-ISAC's Technical Committee exchanges information internally through twice-a-week conference calls, a secure Web site, and encrypted e-mails. The IT-ISAC maintains a Web site for sharing information with the public and internally with its members. A secure portion of its Web site is reserved for ISAC member companies to share information with one other. In addition, the IT-ISAC hosts a daily cyber conference call with US-CERT and the operations centers of other ISACs, as well as a weekly conference call focusing on physical issues with only the operations centers of other ISACs. The Department of Defense (DOD) and the IC also host numerous conference calls and video teleconferences to share information daily.

In addition, other tools provide a means for communicating and exchanging information during crises or emergencies, including programs such as the Critical Infrastructure Warning Information Network (CWIN), Government Emergency Telecommunications Service (GETS), Wireless Priority Service (WPS), and ENS Appendix 4, Protective Programs, provides additional detail about these programs.

4.4 Actions

The following bulleted list includes near term and long term actions to be completed to implement this section of the SSP.

4.4.1 Near Term (~1 year)

Focal Points for Information Sharing

- Coordinate and integrate IT-ISAC and IT SCC efforts by offering recipient IT-ISAC membership to all IT SCC members and defining the roles and responsibilities of each organization to coordinate initiatives more effectively, assign accountability, and minimize duplicative efforts. (*IT-ISAC and SCC*)

- Increase the IT-ISAC's reach by augmenting current recruitment efforts by instituting a partnership program whereby ISAC membership is offered to representatives of IT trade associations and other IT-related organizations. *(IT-ISAC and SCC)*
- Identify and share POC lists to improve the ability to draw on the subject matter expertise available throughout the sector and to interact and coordinate with law enforcement for routine preparedness activities, as well as crisis situations requiring continuity of operations and continuity of government activities. *(SCC, IT-ISAC, GCC, NCSD)*
- Exchange information with the Communications SCC and coordinate on issues related to convergence of the IT and telecommunications infrastructures. Designating an IT SCC representative to serve on the Communications SCC and including a Communications SCC representative on the IT SCC Executive Committee will facilitate the exchange of information. *(SCC)*

Policies and Procedures for Sharing and Reporting Incidents

- Work with State and local governments to refine the security focus of SLFCs and clarify the relationship between SLFCs and the private sector, including clarifying how SLFCs relate to other information-sharing mechanisms sponsored by DHS and how information flows between entities. *(DHS and NCSD with input from SCC and GCC)*
- Develop a Concept of Operations (ConOps) to formalize information sharing within the IT-ISAC's membership and between the IT-ISAC and external organizations, including US-CERT. *(IT-ISAC) (Underway)*
- Develop a Private Sector ConOps to guide US-CERT interaction with the private sector. *(US-CERT with input from the ISAC community and other private sector security partners) (Underway)*
- Develop MOUs to establish, where appropriate and necessary, formal information-sharing agreements at the organizational level to better facilitate data exchange. *(Individual GCC and SCC entities or other security partners as appropriate)*

Procedures for Protecting and Disseminating Sensitive Proprietary Industry Information

- Raise awareness about the PCII Program among Federal, State, and local government and private sector participants and articulate the value that participants in the PCII Program can derive from submitting sensitive information. (DHS PCII Program)
- Assess the use of the PCII Program for submitting sensitive information, including risk management information, to the government. *(SCC, other private sector entities, GCC, and State and local governments)*

Access to Classified and SBU Government Information

- Identify private sector security partners with Federal Government-issued security clearances that should receive government information, and provide their names and pertinent contact information to the DHS and other Federal departments and agencies (e.g., the IC-IRC) to facilitate more timely and extensive sharing of critical and actionable classified intelligence information with appropriately cleared individuals and organizations. *(SCC, IT-ISAC, and NCSD)*
- Identify mechanisms for private sector and State and local government officials who have security clearances to gain access to classified information pertinent to the IT Sector. *(DHS with input from NCSD and NASCIO)*

Mechanisms for Communicating and Disseminating Information

- Identify, update, and maintain appropriate private sector and State and local government POCs who should participate in emergency communication mechanisms such as CWIN, ENS, GETS, and WPS. *(NCSD and NCS with SCC, IT-ISAC, and NASCIO input)*
- Routinely test and exercise processes, procedures, emergency communications systems, and capabilities; document lessons learned; and make recommendations for improvement. *(NCS with NCSD, SCC, and GCC input)*

- Use Homeland Security Information Network for Critical Sectors (HSIN-CS) as a mechanism for exchanging information with IT Sector private sector security partners. As information is made available, the IT-ISAC will pull it from HSIN-CS and push it to IT-ISAC members for their use. (*NCSD and other components of DHS, IT-ISAC*)
- Adopt a common format (e.g., ISAC council template) for presenting information that is shared with the IT Sector private sector security partners. (*NCSD working with other components of the DHS*)
- Develop a strategy to leverage the Homeland Security Information Network (HSIN) to exchange IT Sector information with State and local governments. The strategy may consider duplicating or leveraging the IT-ISAC process of pulling information from HSIN-CS and pushing it to IT-ISAC members. (*NCSD and other components of the DHS with NASCIO input*)

4.4.2 Long Term (1-3 years)

Focal Points for Information Sharing

- Encourage public and private sector security partners to commit to participating in the NIPP partnership model, specifically the ISACs, including the IT-ISAC and MS-ISAC. (*DHS Office of Infrastructure Protection (OIP), NCSD, NCS, and other DHS components*)
- Address areas of convergence, such as those identified in the President's National Security Telecommunications Advisory Committee (NSTAC), NSTAC Report to the President on the National Coordinating Center,[25] including developing an approach for a long-term regional communications and IT coordinating capability that serves all regions of the Nation, convening a conference to focus on cyber issues, and exploring ideas for a multi-industry coordinating center. (*NCSD, NCS, GCC, SCC, Communications SCC, and Communications GCC*)

Policies and Procedures for Sharing and Reporting Incidents

- Undertake an initiative to characterize and map the flow of information between and among security partners for all stages of preparedness activities. This initiative should include information on who shares what information, who receives the information, and what networks and systems are being used to disseminate and exchange the information. (*NCSD and other DHS components with input from SCC, IT-ISAC, and GCC*)

Procedures for Protecting and Disseminating Sensitive Proprietary Industry Information

- Develop the mechanisms and capabilities (e.g., access controls, user rights, and authentication) needed to assure the private sector that its data will be protected. (*NCSD and other DHS components with input from SCC, IT-ISAC, and GCC*)
- Familiarize government entities with IT-ISAC tiered information-sharing mechanisms and capabilities. (*NCSD and IT-ISAC*)

Access to Classified and SBU Government Information

- Explore ways of clarifying the procedures for handling FOUO, SBU, LES, and other sensitive information. (*Homeland Security Council with input from NCSD, SCC, and GCC*)

Mechanisms for Communicating and Disseminating Information

- Design, develop, and implement a protected information-sharing architecture as outlined in the NIPP. (*DHS Office of Infrastructure Protection, Information Sharing Environment*)
- Exercise processes and procedures (e.g., standard operating procedures and ConOps) and communication mechanisms (e.g., HSIN-CS, GETS, CWIN, and WPS) and evaluate lessons learned to enhance information sharing from a cultural, organizational, and technological perspective. (*NCSD, NCS, DHS Office of Infrastructure Protection, SCC, GCC*)

[25] President's National Security Telecommunications Advisory Committee (NSTAC), *NSTAC Report to the President on the National Coordinating Center*, May 10, 2006.

Achieving an enhanced information-sharing framework requires commitment from public and private sector security partners. Participation in the IT SCC and IT GCC requires commitment not only on the part of individual members, but also on the part of the organizations employing them. Implementation of the above actions cannot be achieved without a core group of committed individuals from the public and private sectors. This core group of individuals and organizations may not necessarily be the same as those who were responsible for outlining the vision for an enhanced information-sharing framework. Investment in resources and human capital is necessary for success.

5. CI/KR Protection Research and Development

Over the past several years, several committees and organizations have analyzed and reported on IT Sector security gaps. The result is a substantial body of work describing these gaps and proposing R&D priorities to bridge them. Although each of these analyses is a call to action for a unique audience, the underlying themes, overall conclusions, and resulting objectives are consistent across the board. This section leverages this work to build a structure for IT Sector R&D based on the common themes established by these prior analyses.

Value Proposition

Visibility into R&D priorities and initiatives being undertaken by the private sector and Government break down existing barriers and promote collaboration to ensure that resources are allocated and used efficiently, R&D initiatives are timely, and ultimately products and services are in the pipeline in time to enhance the security of the IT Sector and the Nation.

5.1 Current IT Sector Research and Development

This section describes existing analytical work, identifies common themes among them, and documents new areas of importance not covered previously. The President's Information Technology Advisory Committee's (PITAC) *Cyber Security: A Crisis of Prioritization* (February 2005) and the National Science and Technology Council's (NSTC) *Federal Plan for Cyber Security and Information Assurance R&D* (April 2006) provide a foundation for this section because they are timely and represent two ends of a spectrum in terms of granularity and depth of discussion. In addition, these two reports represent the points of view of private sector experts and the Federal Government. These reports not only convey the thoughts of the authors themselves but also are compilations of the many other previous reports that the authors used to construct their analyses. For example, the PITAC analyzed more than 30 reports to develop its conclusions and 10 areas of prioritization. In addition to these primary references, this section builds on concepts from the following documents to construct the common themes:

- Internet Architecture Board (IAB) Concerns and Recommendations Regarding Internet Research and Evolution, Internet Engineering Task Force, Request for Comments 3869, August 2004
- Grand Research Challenges in Information Security and Assurance, Computing Research Association, November 2003
- The National Strategy to Secure Cyberspace, The White House, February 2003
- The Cyber-Posture of the National Information Infrastructure, RAND Corporation, 1998
- National Cyber Security Research and Development Act (Public Law 107-305), 2002
- Hard Problems List, INFOSEC Research Council, 2005

- The National Plan for R&D in Support of CIP, Office of Science and Technology Policy (OSTP), Executive Office of the President, and Science and Technology (S&T) Directorate, DHS, 2004

Following are the common prioritization themes reflected in these analyses:

- Cyber situational awareness and response;
- Forensics;
- Identity management: authentication, authorization, and accounting;
- Intrinsic infrastructure protocols security;
- Non-technology security issues;
- Control systems security;
- Scalable and composable secure systems;
- Secure coding and software engineering; and
- Trust and privacy.

5.2 IT Sector R&D Priorities

This section presents the IT Sector R&D priorities, which often are consistent with existing studies. However, additional items are included to align these priorities with the overall IT Sector goals. Some of the following factors have influenced this work:

- Greater involvement of the private sector envisioned in the R&D efforts;
- Greater focus of the SSP on elements that can be executed quickly and effectively; and
- SSP time horizon of 1-3 years in terms of completing research projects, or beginning them, even if the eventual delivery horizon is longer.

The IT SCC and IT GCC identified the following IT R&D priorities listed alphabetically:

- **Cyber Situational Awareness and Response.** Research into development of tools and techniques allowing for greater awareness of the state of an IT environment resulting in a timely public and private sector response to factors affecting its security.[26]
- **Forensics.** Research into mechanisms for identifying, tracking, and bringing to justice perpetrators of crimes leveraging cyberspace.[27]
- **Identity Management: Authentication, Authorization, and Accounting.** Research into scalable, user-friendly mechanisms for ensuring access to resources based on the identity of the requestor.[28]
- **Intrinsic Infrastructure Protocols Security.** Research on building security into foundational protocols, such as the DNS, Border Gateway Protocol (BGP), Session Initiation Protocol (SIP), and others on which the information infrastructure is built. This effort includes research toward fundamentally improving the security of relatively new IT technologies, such as wireless and Voice over Internet Protocol (VoIP).[29]

[26] Sections 1.4, 1.5, 1.6, 1.7 and 1.8 of NSTC plan, Functional Cyber Security; sections 5 and 6 of PITAC report, *Monitoring and Detection and Mitigation and Recovery Methodologies*.
[27] Section 1.9 of NSTC plan, Forensics, Trace Back and Attribution; section 4 of PITAC report, *Cyber Forensics: Catching Criminals and Deterring Criminal Activities*.
[28] Section 1.1 of NSTC plan, Authentication, Authorization, and Trust Management; section 4 of PITAC report, *Authentication Technologies*.
[29] Sections 2 and 3 of NSTC plan, Securing the infrastructure and Domain Specific Security; section 4 of PITAC report, *Secure Fundamental Protocols*.

- **Modeling and Testing.** Research on building scalable tools and test beds to develop a greater understanding of the state of currently deployed technologies, as well as the readiness of technologies about to be deployed in the field.[30]
- **Control Systems Security.** Research into improving the security of process control systems and associated information networks that cut across almost all critical segments of society.[31]
- **Scalable and Composable Secure Systems.** Research into the security of larger systems formed by integrating smaller systems to achieve various scalability objectives.[32]
- **Secure Coding, Software Engineering, and Hardware Design Improvement.** Research into improving the way software and hardware are developed to meet needs for reducing vulnerabilities resulting from software and hardware flaws.[33] Technology life cycle assurance mechanisms, including advanced engineering disciplines, standards and certification regimes, and best practices are important to this work. Research areas to focus on include investigation into refining current assurance mechanisms and developing new ones where necessary, developing certification regimes and exploring policy and incentive options. All of these must be provable in terms of demonstrating a reduction in security issues.
- **Trust and Privacy.** Research into ways to ensure that IT systems protect the privacy rights of individuals using IT systems while maintaining overall system security.[34]

5.3 Coordinating IT Sector R&D Priorities

The IT SCC and IT GCC will facilitate awareness and, where possible, coordination of IT security research. The IT GCC is a source of Federal Government expertise and can provide access to individuals and programs responsible for identifying research priorities and managing their implementation. Such facilitation requires engaging multiple partners in the R&D process to pool resources toward the objective of awareness and coordination.

To initiate this process, the IT SCC and IT GCC will establish an R&D Working Group that will engage with research-oriented partner organizations to help implement the proposed initiatives described in this section (see text box), and others as they evolve. The following list includes possible security partners but is not exhaustive; additional entities may be identified as the R&D efforts evolve.

Relevant Federal Government bodies include the following:

- OSTP;
- DHS S&T Directorate;
- Defense Advanced Research Projects Agency;
- National Science Foundation (NSF);
- NIST;
- Naval Research Laboratory;
- President's Committee of Advisors on Science and Technology;

[30] Section 6 of NSTC plan, Enabling Technologies for Cyber Security and Information Assurance R&D; section 8 of PITAC report, *Modeling and Test Beds for New Technologies*.
[31] Section 2.4 of NSTC plan, Secure Process Control Systems.
[32] Section 7.3 of NSTC plan, Composable and Scalable Secure Systems.
[33] Section 5.x of NSTC plan, Foundations for Cyber Security; section 4 of PITAC Report, *Secure Software Engineering and Software Assurance*.
[34] Section 8.x of NSTC plan, Social Dimensions of Cyber Security; section 10 of PITAC report, *Non-Technology Issues That Can Compromise Cyber Security*.

- Interagency Committee on Networking and Information Technology Research and Development;
- National Research Council;
- NSTC;
- U.S. House of Representatives Committee on Science; and
- U.S. Senate Committee on Commerce, Science and Transportation.

Private sector associations include the following:

- Computing Research Association;
- Association of Computing Machinery; and
- Internet2.

Two potential mechanisms for further coordinating IT Sector security research include the establishment of an online clearinghouse for exchanging information and collaborating on IT Sector R&D priorities and conducting an annual IT Sector R&D workshop to provide a means for conducting outreach, reviewing research projects in the pipeline, considering shortfalls in the execution of national research priorities, and reaching consensus on general requirements for government and private sector funding and human resource requirements for ongoing and new research initiatives.

In addition, a common taxonomy for exchanging information on progress toward accomplishing the IT Sector's goals for each R&D priority area can promote an understanding across the IT Sector R&D community and further collaboration activities. The following questions can form the foundation for a common taxonomy:

- **How many projects are underway in pursuit of that priority?** Although quantity is not a comprehensive measure of success, it is important to track the various efforts focused on a given objective.
- **What is the relevance of each project to the goal of the area, and to what extent does each project solve the problem the area identifies?** It is conceivable that some projects would be more relevant than others. It is important to track the relevance of the projects to measure how they affect the desired outcome.
- **What is the potential for each project to result in products that can be transitioned to the field?** This is a test of the project's ability to provide practical solutions.

Potential Coordination Mechanisms

Online Clearinghouse. Establish and maintain a searchable clearinghouse that accomplishes the following:

- Enables individuals and organizations interested in R&D efforts to quickly and easily gauge the state of the art in a particular area of interest;
- Stimulates cross-pollination of ideas from one area of work to another within the IT Sector and between the IT Sector and other sectors;
- Facilitates collaboration within and between public and private sector entities while leveraging their collective efforts and resources; and
- Describes research projects in a common format, and develops and implements processes for gathering, organizing, and maintaining relevant data online.

Projects should be categorized at a high level based on IT Sector R&D priorities. The overall aim would be to provide visibility to public, private, and academic IT security research projects. It is envisioned that current solutions together with enhancements and new developments could provide the foundation for such an online clearinghouse.

Annual IT Sector R&D Workshop. A joint IT SCC and IT GCC annual IT Sector R&D workshop can provide:

- An ongoing mechanism for the IT Sector to gauge the work being done against the priorities it has established;
- A forum where R&D priorities can be discussed and updated by individuals involved in R&D work in various capacities;
- A mechanism to bring private sector and Government together to address common priorities and collaborate on R&D efforts; and
- A forum to highlight and acknowledge the most important work undertaken over the past year toward achieving R&D priorities.

- **At what stage of completion is each project?** This is a measure of the current progress toward achieving the goals of the research area.

It will be important for the government to leverage resources in the private sector to achieve the R&D goals that it shares with the private sector. Leveraging private sector R&D investment while respecting the proprietary nature of some of those efforts is critical to the overall strategy. Demonstrating a value proposition that will motivate the continued and expanded participation of the private sector is a fundamental tenet of the overall SSP process.

5.4 Actions

The following bulleted list includes near term and long term actions to be completed to implement this section of the SSP.

5.4.1 Near Term (~1 year)

- Establish an IT Sector R&D Working Group and identify opportunities for public and private sector security partners to collaborate on R&D priorities. *(NCSD, S&T Directorate, SCC, and GCC)*
- Brief R&D institutions listed above on the SSP to raise awareness of IT Sector R&D priorities, goals and objectives, and risk management approach. *(NCSD, S&T Directorate, SCC, GCC)*
- Coordinate with the Communications Sector on R&D CI/KR protection priorities that overlap or have inherent synergies. *(NCSD, SCC, GCC, NCS, Communications SCC, and Communications GCC)*

5.4.2 Long Term (1-3 years)

- Plan and execute annual IT Sector R&D Workshop and share results with R&D public and private sector security partners. *(SCC and GCC)*
- Develop a 5-year roadmap for IT Sector R&D priorities and resource needs. *(S&T Directorate and NCSD with input from SCC and GCC)*

6. Managing and Coordinating Sector Responsibilities

This section addresses the IT Sector's overall approach for managing and coordinating Sector responsibilities.

Value Proposition

Developing collaborative and coordinated roles and responsibilities for managing IT Sector CI/KR protection activities provides the foundation for open channels of communication among government and the private sector for implementation of the SSP.

6.1 Program Management Approach

HSPD-7 designated the DHS with responsibility for managing and coordinating IT Sector CI/KR protection activities, including leading the development, implementation, and maintenance of the SSP in coordination with the IT SCC and IT GCC. This responsibility has been delegated to NCSD within the DHS's Office of Cyber Security and Communications.

6.2 Processes and Responsibilities

The following sections outline IT Sector processes and responsibilities.

6.2.1 SSP Maintenance and Update

The IT SSP is a living document; consequently, NCSD, IT SCC, and IT GCC representatives will review and update it annually to reflect changes in the sector's security posture and programs. This annual update will leverage the partnership between the IT SCC and IT GCC in developing this plan and will build on the processes used to develop this plan. For example, the IT Sector Plans Working Group will continue to facilitate discussions and dialogue regarding the IT SSP.

The NIPP also will be reviewed triennially by the DHS. NCSD will work closely with the IT SCC, IT GCC, and other security partners to coordinate their participation in the triennial review. Any changes in the NIPP based on the triennial review will be incorporated in the IT SSP annual update.

6.2.2 Annual Reporting

HSPD-7 mandates that each sector shall produce Sector CI/KR Protection Annual Reports to identify, prioritize, and coordinate CI/KR protection in its sector. The NIPP Base Plan provides additional details about these reports. The reports are to be submitted to DHS on July 1 of each year and will describe the sector's CI/KR protection goals, priorities, programs, and related funding, as well as report on progress in the area of CI/KR protection. NCSD will develop the IT Sector CI/KR Protection Annual Report and seek input from the IT SCC and IT GCC to ensure that it accurately reflects the range of sector activities.

6.2.3 Resources and Budgets

Ability to achieve the actions in this plan is dependent on the availability and allocation of resources. Public and private IT Sector security partners make investments and contribute resources (e.g., people, time, and money) to operate critical IT Sector functions and promote the resilience and security of those functions. Because of the sector's diversity and the number of security partners providing resources to secure the sector, neither NCSD nor any other entity has authority over resources and budgets for the entire sector. The NIPP process is designed to prioritize programs and R&D efforts to ensure funding flows to the most critical areas of the IT Sector. The IT GCC and IT SCC will work together to ensure that public and private sector spending reflects the best allocation of available resources.

Managing Sector Resources

IT infrastructure owners and operators ultimately manage their own resources in securing their respective portions of the IT Sector's infrastructure. Federal, State, and local government also manage resources to ensure the availability and resilience of government services. NCSD is responsible for managing some of the Federal Government's resources that support the CI/KR protection of the sector. NCSD will work with other Federal departments and agencies, through the IT GCC, to coordinate priorities for non-SSA funding and resources that support the sector. The private sector can aid in resource allocation decisions by helping the government better understand the resource impact of CI/KR protection and security demands made on the sector and the trickle-down effect on citizens and consumers. Understanding what levels of security investment exceed enterprise capability can help NCSD justify the allocation of resources for national-level capabilities and programs that contribute to the resilience of critical IT Sector functions.

Investment Priorities

Through the IT Sector CI/KR Protection Annual Report, NCSD will identify investment priorities based on risk management priorities, lessons learned, the success of protective programs, and identified needs. NCSD will compile this report in coordination with public and private sector security partners. The report will include priorities and program funding for the current year and projected funding for the following year.

Federal Funding

The annual Federal funding cycle is described below:

- **February Through June:** NCSD coordinates with other DHS components to develop recommendations concerning the DHS budget requests. This request includes funding for IT Sector security-related expenditures that are supported by NCSD and the DHS.
- **September 1:** NCSD submits its budget requests for the following fiscal year.
- **September Through November:** NCSD, through DHS headquarters, works with OMB to make final decisions regarding the DHS budget and resources available for the division and specific IT Sector programs.

6.2.4 Training and Education

Training and education are crucial to maintaining individual and organizational CI/KR protection expertise and to implementing the risk management framework successfully. Rapid changes in technology (e.g., the growth of e-learning) affect how training is delivered and what competencies are needed (e.g., the growing need for information security skills). An important component of a comprehensive IT security workforce development program is the enhancement and professionalization of the individuals currently involved in IT security operations and program management. A recently completed study estimated that there are 1.5 million information security professionals throughout the world.[35] Of this total, approximately 40 percent are employed in the U.S. and Canada. IT security has become a separate and distinct career field. The continuing education and

[35] Allan Carey, IDC White Paper: 2006 Global Information Security Workforce Study, October 2006.

development of the current IT security workforce is an important aspect of the initiative to improve the security posture of the nation's IT infrastructure.

- **National Centers of Academic Excellence in Information Assurance Education (CAEIAE).** The CAEIAE program, founded in 1998 by the National Security Agency (NSA), has been co-sponsored by DHS since 2004. The program is open to 4-year colleges and universities that demonstrate significant depth and maturity in their information assurance (IA) programs. CAEIAEs must map portions of their security curricula to at least two IA standards from the Committee on National Security Systems. The schools may reapply every 3 years to be redesignated as CAEIAEs. As of December 2006, 75 schools in 32 States and the District of Columbia are designated. The CAEIAE program plans to have at least one center in every State.
- **Federal Cyber Service: Scholarship For Service (SFS).** The SFS program, originally established by NSF in 2001, has been co-sponsored by DHS since 2004. This program provides scholarship money for a maximum of 2 years to outstanding cyber security undergraduate, graduate, and doctoral students in exchange for an equal amount of time spent in Federal Government service after graduation. Eligible students must attend a university or college designated as a CAEIAE. As of December 2006, 30 institutions are participating in the SFS program.
- **Project MBA.** NCSD and DHS's Risk Management Division (RMD) launched Project MBA in January 2006 as an effort to incorporate elements of physical and cyber security in business school curricula. The pilot program, which takes place at George Mason University's School of Management, includes simulations, lectures, and discussions on topics such as emergency preparedness, business continuity planning, and cyber security. Based on feedback from the pilot, the program may be expanded to additional graduate business schools during the 2007 academic year.
- **Professional Certifications.** Professional certifications have become recognized as an important qualification for individuals who chose IT security as their career field. Over the past ten years the number of individuals attaining a professional IT security certification has grown dramatically. This growth reflects not only the rapid increase of individuals entering the IT security field, but also growth in the number and diversity of available certifications. These now range from highly technical, vendor specific credentials to those which cover the broad spectrum of information security in a product neutral manner.
- **Department of Defense IT Security Workforce Enhancement Program.** The Department of Defense (DOD) has recognized that a critical factor in improving the security of their information systems infrastructure is the development of a skilled, professional IT security workforce. DOD has established a fundamental requirement that all employees (i.e., active duty and reserve military, civilian personnel—to include foreign nationals, and contractors) who have privileged access to a DOD system, or are involved in security management, must attain professional certification by the end of fiscal year 2010. The Department estimates that this requirement will apply to approximately 100,000 individuals. DOD has approved various "commercial" certifications as meeting their requirements in both the managerial and technical tracks.
- **Other Professional Development Activities.** As the IT security profession matures, there is growing recognition of the need to maintain and enhance their technical and managerial skills. Numerous conferences and educational events are held each year that cover various aspects of the IT security problem. These provide an opportunity for individuals in the public and private sectors to exchange information in a collaborative environment. In addition, there has been a growth in professional associations that provide educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of their members.
- **Exercises.** Tabletop and full-scale exercises fulfill many training and education objectives. In addition to supporting specialized training for individuals, exercises support cross-sector training, as well as general outreach and awareness. For example, NCSD sponsors the National Cyber Exercise (Cyber Storm) series, which strengthens preparedness, response, coordination, and recovery mechanisms within Federal, State, and local governments, and in conjunction with the private sector. In accordance with congressional mandates to conduct exercises that test response to cyber attacks on critical infrastructures, the exercise meets HSPD-8, National Preparedness, requirements. It is coordinated with the DHS National Exercise Program.

The National Cyber Exercises provide the venue for the DHS; the SSAs; other Federal agencies; the private sector; and State, local, and tribal government entities to identify interdependencies, integrate infrastructure protection activities within other national-level plans, identify overlaps, rectify gaps, and establish mechanisms for coordination and information exchange. The National Cyber Exercise sponsors collaborate with various security partners throughout the coordination, planning, and execution of an exercise. The private sector is one of the most significant security partners for the National Cyber Exercises. Because the private sector owns or operates more than 85 percent of the critical infrastructure, its involvement in the planning process and execution of any CI/KR exercise is inherently crucial to its success. NCSD works closely with the IT SCC and IT-ISAC to facilitate and promote private sector involvement in its exercises.

- **Future Plans and Initiatives.** Training and education is a continuous process and is a responsibility of the public and private sectors. Future CI/KR protection training and education efforts are focused on aligning training programs with IT Sector goals and objectives; identifying and assessing standard training needs for the entire sector; allocating training resources from the private and public sectors; designing and delivering standard training for the sector; and evaluating training.

In addition, owners, operators, and other IT Sector entities conduct internal training and fund vendor-neutral certifications to ensure that their employees are appropriately trained. Examples of internal training include training related to risk assessments, risk management, cost-benefit analysis, and related concepts.

6.3 Roles and Responsibilities

The following sections outline SSA, SCC, GCC, and shared responsibilities.

6.3.1 Sector-Specific Agency

NCSD has responsibility for working with public and private IT Sector security partners to promote not only the physical, human, and cyber elements of the infrastructure but also the cyber security of all infrastructure sectors as consumers of IT. NCSD responsibilities are as follows:

- **Coordinate development and drive implementation of the IT SSP:**
  - Coordinate efforts to compose and maintain the IT SSP;
  - Support implementation of the collaboratively developed risk assessment approach for the IT Sector;
  - Coordinate efforts to determine protective measures for the IT Sector;
  - Identify R&D requirements and conduct R&D in concert with other government entities, the private sector, and other security partners;
  - Ensure public and private sector security partners are engaged, as early as possible, in the development and revision of the SSP and in planning other CI/KR protection initiatives;
  - Encourage and promote participation in the IT GCC, IT SCC, and IT-ISAC; and
  - Support the IT-ISAC as the operational information-sharing mechanism for the private sector.
- **Engage with IT Sector security partners:**
  - Identify relevant public and private sector security partners that have a role in securing the IT Sector;
  - Develop a plan for regular engagement between NCSD and the public and private IT Sector security partners;

– Promote security awareness within the IT Sector;

– Communicate timely, analytical, and useable information, including threat and warning information, specific to the infrastructure and public and private IT Sector security partners;

– Identify incentives for the private sector to undertake voluntary efforts to improve security (physical, cyber, and human) and implement the SSP;

– Encourage the use of risk transfer mechanisms, such as contractual arrangements that expand the use of state-of-the-art security practices through market mechanisms; and

– Develop a business case for continuing investment in securing the IT Sector.

- **Engage with other government entities:**

  – Work with the intelligence and law enforcement communities to enhance the collection, assessment, and distribution of cyber-related intelligence to IT Sector security partners;

  – Solicit input from government entities on IT Sector CI/KR protection-related efforts;

  – Work with US-CERT to provide cyber alerts, response assistance, and information on remediation measures to public and private sector security partners; and

  – Interact with other SSAs and sectors to identify unique dependencies, interdependencies, relationships, and partnerships across sectors.

6.3.2 IT Sector Coordinating Council[36]

The IT SCC's responsibilities are as follows:

- **Develop and drive implementation of the IT SSP:**

  – Participate in the development, review, and enhancement of the IT SSP;

  – Support the identification and risk assessment of critical IT Sector functions;

  – Collaborate with NCSD and other public IT Sector security partners to identify current and future protective program needs;

  – Encourage and share advances in security resulting from R&D; and

  – Use the IT-ISAC as the focal point for operational information sharing with the private sector.

- **Engage with IT public sector security partners to promote CI/KR protection:**

  – Identify relevant public sector security partners that have a role in securing the IT Sector; and

  – Promote security awareness within the IT Sector.

6.3.3 IT Government Coordinating Council[37]

The IT GCC has responsibility for coordination of strategies, activities, policy, and communications across government entities with a role in securing the IT Sector. The IT GCC's responsibilities are as follows:

- Develop and facilitate implementation of the IT SSP:

  – Lead efforts to develop, review, enhance, and maintain the IT SSP;

[36] For a complete list of IT SCC members, see section 1.4

[37] For a complete list of IT GCC members, see section 1.4.

– Support the identification and risk assessment of critical IT Sector functions;

– Collaborate with private IT Sector security partners to identify current and future IT Sector protective program needs; and

– Encourage and share advances in security resulting from R&D.

- **Engage with IT private sector security partners to promote CI/KR protection:**

  – Identify relevant private sector security partners that have a role in the security of the IT Sector;

  – Participate in the sector partnership model to coordinate with IT Sector security partners;

  – Use available communication tools (e.g., HSIN-CS, Web site, and telephone hotline) to exchange information with the private sector in relation to the IT Sector; and

  – Promote security awareness within the IT Sector.

6.3.4 Shared Cross-Sector Cyber Security Responsibilities

Various critical IT Sector functions are consumed by other critical infrastructure sectors and by Federal, State, and local governments. The IT Sector provides the ability to secure IT products and services; however, each sector is individually responsible for the day-to-day operational security of its cyber systems. The IT Sector has an understanding of not only how its products and services are used by consumers, but also an understanding of the security challenges that other sectors face as they use their cyber infrastructure. Public and private IT Sector security partners leverage this expertise to assist other CI/KR sectors and governments in addressing cyber security.

6.4 Actions

The following bulleted list includes near term and long term actions to be completed to implement this section of the SSP.

6.4.1 Near Term (~1 year)

- Update the IT SSP annually. (*GCC and SCC*)
- Develop (annually) the IT Sector CI/KR Protection Annual Report. (*NCSD with GCC and SCC input*)
- Identify necessary resources to implement the IT SSP risk management approach, protective programs, information sharing mechanisms, R&D initiatives, and performance measurement. (*NCSD, GCC, and SCC*)
- Engage with and develop public sector programs to support the implementation and maintenance of the IT SSP. (*NCSD*)
- Coordinate closely with the Communications Sector on the development of the next Communications SSP. (*GCC and SCC*)

6.4.2 Long Term (1-3 years)

- Develop and facilitate training and education initiatives necessary to implement the IT SSP successfully. (*NCSD, GCC, and SCC*)
- Collaborate with the Communications Sector on outreach and education to customers on their reliance on Communications and IT infrastructures and security roles and responsibilities. (*NCSD, GCC, SCC, NCS, Communications SCC, and Communications GCC*)
- Fulfill the roles and responsibilities identified in section 6.3. (*All*)

7. Implementing the SSP and Tracking Progress

Tracking the implementation progress of the actions set forth in this plan is essential to the SSP's success. A collaborative process that benefits from the voluntary input of IT SCC and IT GCC representatives can most accurately track the SSP's implementation. Tracking SSP implementation provides public and private sector security partners with a shared understanding of the progress toward achieving the sector's goals. This section describes the IT Sector's demonstration of successful SSP implementation in support of its goals and objectives.

7.1 Tracking Progress Challenges

The IT SSP contains clear goals and objectives supported by specific action items. Implementing those action items in support of sector goals and objectives is a responsibility shared by public and private sector security partners. Implementing and tracking the action items requires commitment and resources (e.g., financial, time, personnel, and specific expertise) from the public and private sectors. Dedicated financial and personnel resources also may be required to implement and accurately track the progress of the SSP. Public and private sector security partners will need to prioritize the actions in this plan and proceed with implementation and tracking using an iterative approach that takes resource availability into account.

7.2 Measurement Overview

The IT Sector has a diverse operating environment that is marked by continuous evolution, convergence, and heterogeneous architectures, networks, technologies, and businesses. With such diversity across the IT infrastructure, security partner base, and key functions, traditional quantitative measurement approaches are not ideally suited to the IT Sector. For example, a quantitative measure to assess the risk mitigation efforts of ISPs would have little utility for assessing the risk mitigation efforts of IT system integrators. Therefore, the IT Sector's approach will rely on qualitative, implementation-focused measurement. The IT Sector focuses on identifying and tracking public and private sector progress in implementing SSP action items. The IT Sector's approach will track the sector's progress toward achieving its goals with respect to four key categories:

- **One-time activities described in the IT SSP.** These are one-time SSP action items (e.g., implementing a specific protective program).
- **Recurring activities described in the IT SSP.** These are recurring SSP activities (e.g., reports and conferences).
- **Private sector self-directed activities.** These are activities undertaken by the IT industry that are outside the scope of the SSP, but still contribute to the overall IT Sector goals (e.g., security standards development).

- **Public sector self-directed activities.** These are activities undertaken by Federal, State, and local governments that are outside the scope of the SSP but still contribute to the overall IT Sector goals.

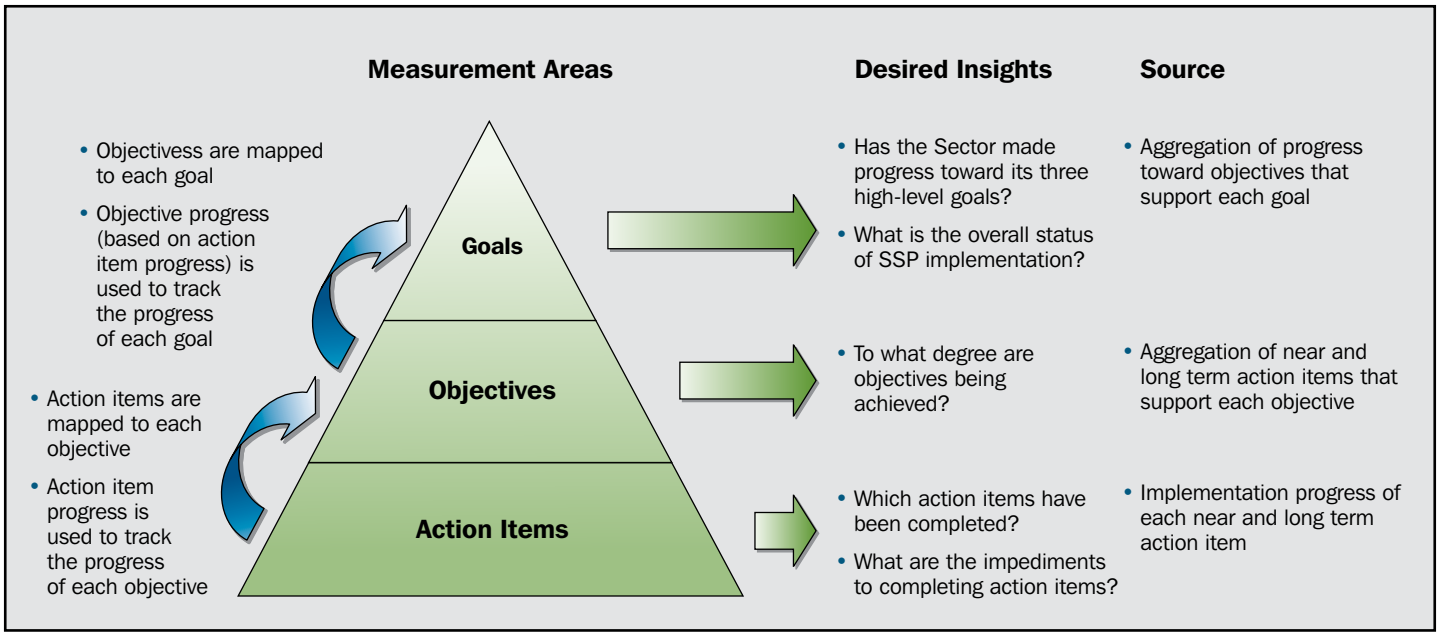
All suggested SSP action items support the sector's goals. Therefore, implementation of action items serves as an indicator of progress toward a sector goal.

7.3 Measurement Approach

The IT Sector's approach will track progress against sector goals iteratively. As figure 7.1 illustrates, the near- and long-term action items described in each section and the public and private sector self-directed activities will serve as the foundation of the sector's measurement approach.

As also shown in figure 7-1, the measurement approach is hierarchical—each action is mapped to a specific sector objective, which is mapped to a sector goal. Therefore, each objective is met when the action items that support it are implemented. Thus, an evaluation of the implementation of the action items yields insights into the support of each objective. Similarly, the implementation of each objective yield insight into the progress the sector has made toward each goal. By using this approach, NCSD, the IT SCC, and IT GCC can gain insights into implementation progress and provide actionable outputs that can guide sector activities to ensure that goals are being supported.

Figure 7-1: IT Sector Measurement Approach

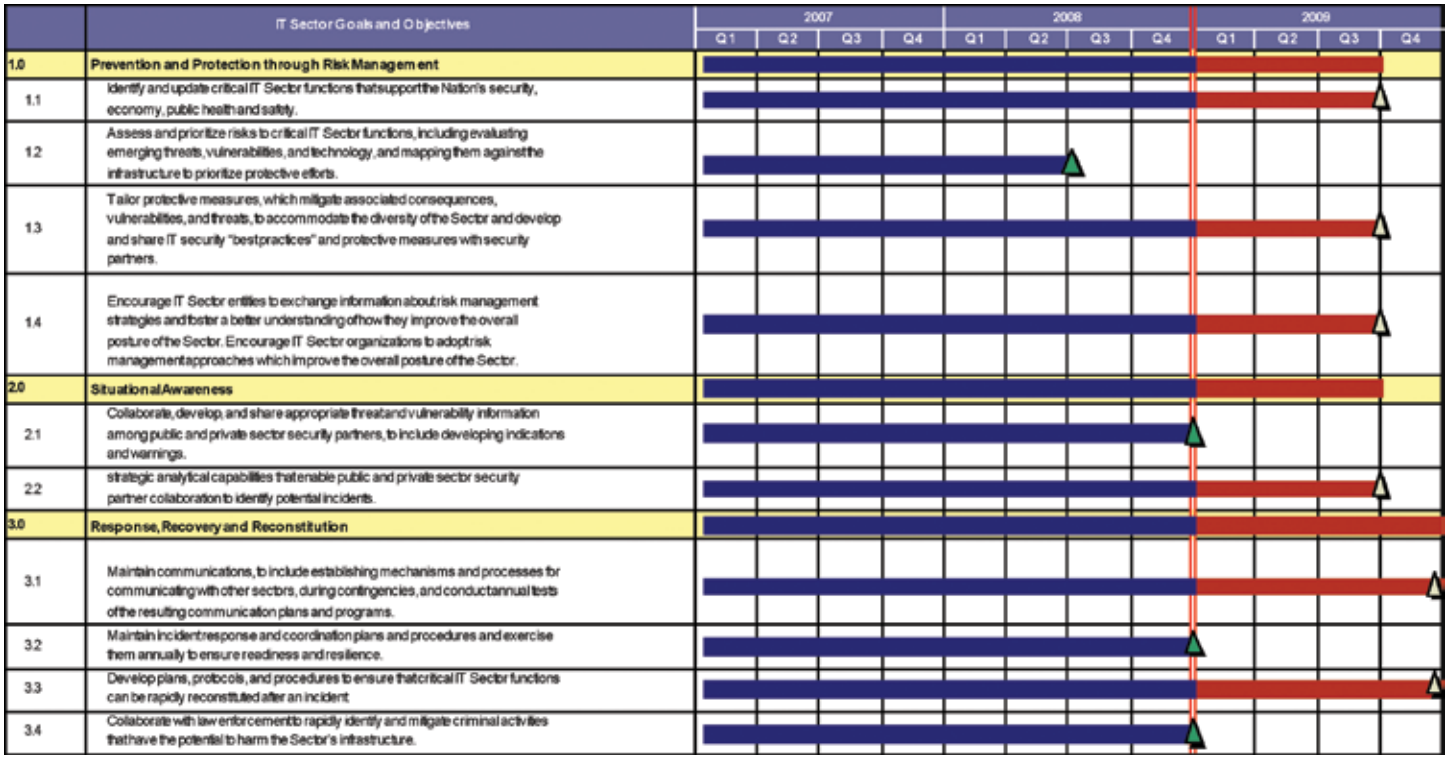


7.4 Goals and Objectives Measurement

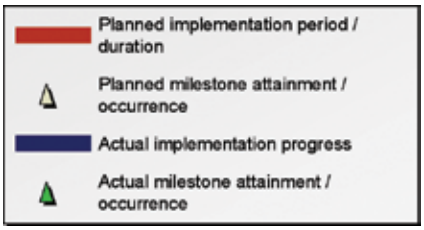
To illustrate implementation levels and goal support, the IT SCC and IT GCC will rely on Gantt charts to show activity, duration, and completion. A Gantt chart is a modified bar chart that shows duration and milestones of key activities within a project framework.

Figure 7-2 is a notional Gantt chart to track IT SSP implementation at the highest level of the measurement hierarchy—goals and objectives. Figure 7-2 illustrates how IT Sector progress could be reported in future iterations of the SSP or for IT Sector CI/KR Protection Annual Report purposes—in this example, at the end of the fourth quarter (Q4) of 2008. Objective 1.1 provides a hypothetical example of how activities that support objective 1.1 may have been implemented from Q1 2007 through Q4 2008. The planned duration of implementation is through Q3 2009, as indicated by the beige triangle. Objective 1.2 illustrates that all activities were implemented from Q1 2007 through Q2 2008, which concluded all required actions for objective 1.2 as indicated by the green triangle. The overall performance of goal 1 implementation is measured in row 1.1 and is a product of the implementation of the activities supporting the objectives that support goal 1.

Figure 7-2: Notional Gantt Chart to Indicate Goal and Objective Implementation Progress at Q4 2008



By observing the planned and actual implementation periods and milestones, the IT SCC and IT GCC can determine the implementation progress of SSP action items. The level of implementation then can be used to determine the extent to which the sector is achieving its goals.



7.5 Activities Implementation

The goals and objectives implementation measures are an aggregation of the implementation of near-and long-term activities from across four categories:

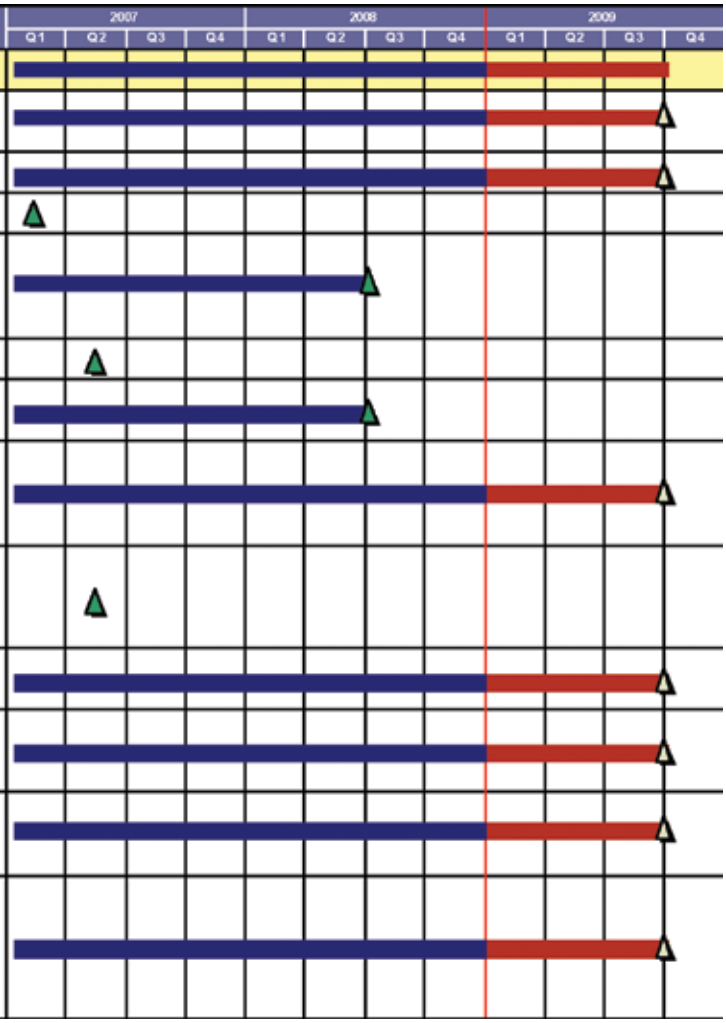
- One-time activities described in the IT SSP;
- Recurring activities described in the IT SSP;
- Private sector self-directed activities; and
- Public sector self-directed activities.

Together, NCSD, the IT SCC, and IT GCC will develop Gantt charts that illustrate the implementation progress of sector activity across the four categories outlined above, each mapped to a specific objective and goal. Figure 7-2 displays a notional Gantt chart that illustrates the type of detail that will be offered. Note that figure 7-3 provides more granular details about the information presented in figure 7-2 by illustrating the implementation levels of each activity that support the Objectives.

For example, figure 7-3 shows that activity 1.1.1 is a *recurring activity* identified in the SSP that has been continually implemented from Q1 2007 through Q4 2008 and has a planned conclusion date of Q3 2009. In addition, activity 1.1.2 was a *one-time activity* that was completed in Q1 2007. Thus, overall, Objective 1.1 has been continually implemented since Q1 2007 and is planned to conclude in Q3 2009. Similarly, all activities that support the objectives under goal 1 are on schedule as of Q4 2008 and all are planned to be completed by Q3 2009. Figure 7-3 shows the progression from *action item* to *objective* to *goal* and provides a granular view of how the sector is implementing actions to support its goals. Once the measurement approach is implemented, subsequent SSP iterations will contain progress updates and associated next steps based on the sector's progress tracking activities.

Figure 7-3: Notional Gantt Chart to Indicate Activity Implementation Progress at Q4 2008

	IT Sector Goals and Objectives	One-Time or Recurring	Source
1.0	**Prevention and Protection through Risk Management**		
1.1	Identify and update critical IT Sector functions that support the Nation's security, economy, public health and safety.		
1.1.1	*Annually review and revise CINS definition and process for declaring a CINS.*	*Recurring*	*SSP*
1.1.2	*Decompose the sector's critical functions and/or sub-functions.*	*One-Time*	*SSP*
1.2	Assess and prioritize risks to critical IT Sector functions, including evaluating emerging threats, vulnerabilities, and technology, and mapping them against the infrastructure to prioritize protective efforts.		
1.2.1	*Develop an implementation plan for the 2007 IT Sector Risk Profile.*	*One-Time*	*SSP*
1.2.2	*Initiate the identification and assessment of vulnerabilities and consequences for critical IT Sector functions.*	*Recurring*	*SSP*
1.3	Tailor protective measures, which mitigate associated consequences, vulnerabilities, and threats, to accommodate the diversity of the Sector and develop and share IT security "best practices" and protective measures with security partners.		
1.3.1	*Establish the joint IT SCC and IT GCC Protective Program Working Group to review existing protective programs, identify private sector protective programs, and refine and consolidate the list of current programs.*	*One-Time*	*SSP*
1.3.2	*Hold annual meeting on protective programs before developing the IT Sector CIKR Protection Annual Report.*	*Recurring*	*SSP*
1.4	Encourage IT Sector entities to exchange information about risk management strategies and foster a better understanding of how they improve the overall posture of the Sector.		
1.4.1	*Encourage public and private sector security partners to commit to participating in the NIPP Partnership Model, specifically the ISACs, including the IT-ISAC and MS-ISAC.*	*Recurring*	*SSP*
1.4.2	*Exercise processes and procedures (e.g., standard operating procedures and CONOPs) and communication mechanisms (e.g., HSIN-CS, GETS, CWIN, and WPS) and evaluate lessons learned to enhance information sharing from a cultural, organizational, and technological perspective.*	*Recurring*	*SSP*



7.6 Reporting on Progress

Tracking the implementation progress of actions within this SSP will require the commitment and resources of the IT SCC and IT GCC. The IT SCC and IT GCC will use the following approach for accurate tracking of the implementation progress of action items contained within the SSP:

- As noted in this SSP, each action item has an entity/organization who will be the party responsible for its implementation (e.g., IT-ISAC, NCSD, GCC, and SCC).
- Responsible parties will monitor progress of their action items within the SCC or GCC.
  - For each private sector (IT SCC) action item:
    - The IT SCC (as the lead policy arm) will examine each SSP action item that falls under its purview and will decompose it into measurable components to assess its implementation progress; and

- The IT SCC will collect progress information about each SCC action item from members at IT SCC meetings and aggregate the information to the level of the notional Gantt chart in figure 7-3.

– For each public sector (IT GCC) action item:

- As appropriate, the IT GCC will examine each action item that falls under its purview and decompose it into measurable components to assess its implementation progress; and
- NCSD will collect progress information on each IT GCC-related action item from members at IT GCC meetings and aggregate the information to the level of the notional Gantt chart in figure 7-3.

– For action items that require joint public and private sector collaboration:

- The IT SCC and IT GCC will examine each such action item and decompose it into measurable components to assess its implementation progress; and
- The IT SCC and IT GCC will collect progress information on each such action item from their constituencies at IT SCC and IT GCC meetings and collectively aggregate the information to the level of the notional Gantt chart in figure 7-3.

• The IT SCC and IT GCC will combine their progress data to track overall SSP progress for reporting purposes (i.e., IT Sector CI/KR Protection Annual Report) and for subsequent SSP iterations.

7.7 Actions

The following bulleted list includes near and long term actions to be completed to implement this section of the SSP.

7.7.1 Near Term (~1 year)

• Prioritize sector action items, taking into consideration available resources. *(NCSD, SCC, GCC)*

• Create Gantt chart for the sector that maps SSP actions to objectives and goals. *(NCSD with input from SCC and GCC)*

7.7.2 Long Term (1-3 years)

• Continue to reassess action item prioritization based on evolving status of the sector and resource availability. *(NCSD, SCC, and GCC)*

• Track sector action item progress and update the IT SSP. *(NCSD, SCC, and GCC)*

Appendix 1: List of Acronyms and Abbreviations

APWG	Anti-Phishing Working Group
AT-SPI	Anti-Tamper–Software Protection Initiative
BGP	Border Gateway Protocol
CAEIAE	National Centers of Academic Excellence in Information Assurance Education
CALEA	Communications Assistance for Law Enforcement Act
CARC	Community Acquisition Risk Center
CCIPS	Computer Crimes and Intellectual Property Section
CCEVS	Common Criteria Evaluation and Validation Scheme
CFIUS	Committee on Foreign Investment in the United States
CI	Counterintelligence
CIDDAC	Cyber Incident Detection Data Analysis Center
CII Act	Critical Infrastructure Information Act of 2002
CI/KR	Critical Infrastructure and Key Resources
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIPAC	Critical Infrastructure Partnership Advisory Council
COBIT	Control Objectives for Information and Related Technology
COD	Common Operating Database
ConOps	Concept of Operations
COP	Common Operating Picture
COTS	Commercial Off-the-Shelf
CVE	Common Vulnerabilities and Exposures
CWIN	Critical Infrastructure Warning Information Network
DC3	Defense Cyber Crime Center
DOD	Department of Defense
DCFL	DOD Computer Forensics Laboratory
DCCI	DOD Cyber Crime Institute
DCITP	DOD Computer Investigations Training Program
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DNS	Domain Name System
DOJ	Department of Justice
DPA	Defense Production Act
DRII	Disaster Recovery Institute International
ECPA	Electronic Communications Privacy Act
ECTF	Electronic Crimes Task Forces
EO	Executive Order
ESF	Emergency Support Function
FBI	Federal Bureau of Investigation
FCPA	Foreign Corrupt Practices Act
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only

GCC	Government Coordinating Council
GETS	Government Emergency Telecommunications Service
GFIRST	Government Forum of Incident Response and Security Teams
GLBA	Gramm-Leach-Bliley Act
GSA	General Services Administration
GTLD	Generic Top Level Domain
HIPPA	Health Insurance Portability and Accountability Act
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HSIN	Homeland Security Information Network
HSIN-CS	Homeland Security Information Network for Critical Sectors
HSOC	Homeland Security Operations Center
HSPD	Homeland Security Presidential Directive
IA	Information Assurance
IAB	Internet Architecture Board
IAD	Information Assurance Directorate
IC	Intelligence Community
IC-IRC	Intelligence Community Incident Response Center
ICT	Information and Communication Technology
IDWG	Internet Disruption Working Group
IEC	International Electrotechnical Commission
IEEPA	International Emergency Economic Powers Act
IFCC	Internet Fraud Complaint Center
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center
ISE	Information Sharing Environment
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ISP	Internet Service Provider
IT	Information Technology
ITGI	Information Technology Governance Institute
IT-ISAC	Information Technology Information Sharing and Analysis Center
ITIL	Information Technology Infrastructure Library
IWWN	International Watch and Warning Network
LES	Law Enforcement Sensitive
MOU	Memorandum of Understanding
MS ISAC	Multi-State Information Sharing and Analysis Center
NASCIO	National Association of State Chief Information Officers
NCC	National Coordinating Center
NCIX	National Counterintelligence Center
NCRCG	National Cyber Response Coordination Group
NCS	National Communications System
NCSD	National Cyber Security Division
NDAC	Network Design and Analysis Center
NIAP	National Information Assurance Partnership
NICC	National Infrastructure Coordination Center
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NISAC	National Infrastructure Simulation and Analysis Center
NIST	National Institute of Standards and Technology
NOC	National Operations Center
NRP	National Response Plan
NS/EP	National Security and Emergency Preparedness
NSA	National Security Agency
NSF	National Science Foundation
NSIE	Network Security Information Exchanges
NSTAC	National Security Telecommunications Advisory Committee
NSTC	National Science and Technology Council
NTAC	National Threat Assessment Center

NTOC	National Security Agency Threat Operations Center
NVD	National Vulnerability Database
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OECD	Organisation for Economic Co-operation and Development
OGC	Office of Government Commerce (United Kingdom)
OIP	Office of Infrastructure Protection
OMB	Office of Management and Budget
OSTP	Office of Science and Technology Policy
OVAL	Open Vulnerability Assessment Language
PC	Personal Computer
PCII	Protected Critical Infrastructure Information
PCIS	Partnership for Critical Infrastructure Security
PDD	Presidential Decision Directive
PITAC	President's Information Technology Advisory Committee
POC	Point of Contact
PSN	Public Switched Network
PSTN	Public Switched Telephone Network
R&D	Research and Development
RFI	Request for Information
RISS	Regional Information Sharing System
RMD	Risk Management Division
ROI	Return on Investment
S&T	Science and Technology
SBU	Sensitive But Unclassified
SCC	Sector Coordinating Council
SFS	Federal Cyber Service: Scholarship For Service
SHIRA	Strategic Homeland Infrastructure Risk Assessment
SIP	Session Initiation Protocol
SLFC	State and Local Fusion Center
SLGCP	State and Local Government Coordination and Preparedness
SME	Subject Matter Expert
SOX	Sarbanes-Oxley Act
SSA	Sector-Specific Agency
SSE-CMM®	Systems Security Engineering-Capability Maturity Model
SSP	Sector Specific Plan
TLD	Top Level Domain
TOPOFF	Top Officials
TSP	Telecommunications Service Priority
U.S.	United States
US-CERT	United States Computer Emergency Readiness Team
USSS	United States Secret Service
VoIP	Voice over Internet Protocol
WebEOC	Web Emergency Operations Center
WMD	Weapon of Mass Destruction
WPS	Wireless Priority Service

Appendix 2: Authorities

Key authorities for the IT Sector address the establishment of the IT Sector, its availability, resilience, and security, and provide guidance on sector coordination and specific programs. This appendix provides a brief description of major authorities with relevance to IT Sector CIP activities.

Homeland Security/National Security IT Authorities

- **The Homeland Security Act of 2002** (November 2002). The Homeland Security Act established the following specific CI/KR protection roles and responsibilities for the DHS:
  - Developing a comprehensive national plan for securing the CI/KR of the United States;
  - Providing crisis management in response to attacks on critical information systems;
  - Providing technical assistance to the private sector and other government entities with respect to emergency recovery plans for failures of critical information systems; and
  - Coordinating with other agencies of the Federal Government to provide specific warning information and advice about appropriate protective measures and countermeasures to State, local, and nongovernmental organizations.
- **HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection** (December 2003). HSPD-7 establishes a national policy for Federal departments and agencies to identify and prioritize U.S. CI/KR and to protect them from attack. HSPD-7 identified Telecommunications and IT as distinct sectors and assigned oversight for both to the DHS: NCS serves as the lead DHS agency for the Telecommunications Sector, and NCSD serves as the lead agency for the IT Sector. Specifically, HSPD-7 charges the DHS with maintaining an organization—NCSD—to serve as a focal point for the security of cyberspace and facilitate interactions and collaborations between and among Federal departments and agencies, State and local governments, the private sector, academia, and international organizations. The NCSD mission includes analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems. NCSD supports the Department of Justice (DOJ) and other law enforcement agencies in their continuing missions to investigate and prosecute threats to and attacks against cyberspace, to the extent permitted by law. To the extent permitted by law, Federal departments and agencies with cyber expertise, including the Departments of Justice, Commerce, Treasury, Defense, Energy, and State, and the Central Intelligence Agency, will collaborate with and support NCSD in accomplishing its mission.
- **Intelligence Reform and Terrorism Prevention Act of 2004** (December 2004). This act represents the most dramatic reform to the Nation's intelligence capabilities since the National Security Act of 1947. This authority requires the President

to establish an information-sharing environment (ISE) to facilitate the sharing of terrorism information among all appropriate Federal, State, regional, local, and tribal government and private sector entities, through the use of policy guidelines and technologies; to include provisions for privacy and civil liberty rights; to establish programs for the enhancement of public safety communications interoperability; and to recommend that the DHS promote the adoption of voluntary national preparedness standards for the private sector. The act and subsequent authorization legislation established the position of the Director of National Intelligence (DNI) and give the DNI and DNI/Chief Information Officer (CIO) significant additional authorities and responsibilities regarding the management of the IC and its role in critical infrastructure protection.

- **Presidential Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements in Support of the Information-Sharing Environment** (December 2005). This Presidential memorandum outlines information-sharing authorities and directs executive departments and agencies, in consultation with the program manager for information sharing, to leverage ongoing information-sharing efforts in development of the ISE and to promote a culture of information sharing. In addition, this memorandum provides the following guidelines for the ISE: define common standards for how information is acquired, accessed, shared, and used within the ISE; develop a common framework for the sharing of information between and among executive departments and agencies and State, local, and tribal governments, law enforcement agencies, and the private sector; standardize procedures for SBU information; facilitate information sharing between executive departments and agencies and foreign partners; and protect the information privacy rights and other legal rights of Americans.
- **Executive Order (EO) 13311 (as amended by EO 13388), Homeland Security Information Sharing** (October 2005). This EO creates an ISE to facilitate the sharing of terrorism information and restructures the Information Sharing Council.
- **Executive Order 13353, Establishing the President's Board on Safeguarding American's Civil Liberties** (August 2004). This EO further strengthens protections for the rights of Americans, including freedoms, civil liberties, and information privacy guaranteed by Federal law, in the effective performance of national security and homeland security functions. Accordingly, this EO establishes the President's Board on Safeguarding Americans' Civil Liberties, chaired by DOJ, which advises the President on information-sharing policy issues.
- **HSPD-5, Management of Domestic Incidents** (February 2003). This directive enhances the United States' ability to manage domestic incidents by establishing a single, comprehensive NRP. HSPD-5 places initial responsibility for domestic incident management on State and local authorities but states that the Federal Government will become involved when State and local resources are overwhelmed or Federal interests are involved. This directive also recognizes the role played by private and nongovernmental sectors in preventing, preparing for, responding to, and recovering from terrorist attacks, major disasters, and other emergencies, and orders the Secretary of Homeland Security to coordinate with private and nongovernmental sectors to ensure adequate planning, equipment, training, and exercise activities, and to promote partnerships to address incident management capabilities.
- **HSPD-8, National Preparedness** (December 2003). This directive establishes policies to strengthen the preparedness of the United States to prevent and respond to 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 preparedness capabilities of Federal, State, regional, local, and tribal entities.
- **HSPD-9, Bio Defense Strategy** (April 2004). This directive establishes national policy that prioritizes the protection of critical infrastructure (physical and cyber) from the effects of biological weapons attacks. A biological weapons attack might deny access to essential facilities and response capabilities. Therefore, it is necessary to improve the survivability and ensure the continuity and restoration of operations of critical infrastructure sectors following biological weapons attacks. Assessing the vulnerability of this infrastructure—particularly, the medical, public health, food and agriculture, water, energy, and transportation sectors—is the focus of current efforts. The DHS, in coordination with other appropriate Federal departments and

agencies, leads these efforts, which include developing and deploying biodetection technologies and decontamination methodologies. This HSPD is relevant because human elements of critical IT Sector functions exist. If this human element were affected by a biological attack, cascading effects might occur. For example, if an antivirus vendor organization's campus were affected, the skills and knowledge needed to perform virus definition updates and patching potentially might be unavailable during a crucial time.

- **HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors** (August 2004). This directive establishes national policy to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees). Secure and reliable forms of identification for purposes of this directive means identification that: (1) is issued based on sound criteria for verifying an individual employee's identity; (2) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (3) can be rapidly authenticated electronically; and (4) is issued only by providers whose reliability has been established by an official accreditation process. IT Sector technologies and infrastructure facilitate the implementation of this directive, and future developments in the sector can affect efforts to maintain the common identification standard.
- **Executive Order (EO) 13231 (as amended by EO 13286 as of February 2003), Critical Infrastructure Protection in the Information Age** (October 2001). This EO ensures the protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems in the information age.
- **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001** (October 2001). This act affects companies' IT departments because they must be prepared to provide terrorism-related information to the FBI if subpoenaed.
- **Export Administration Act of 1979, as amended (EAA),** implemented through the Export Administration Regulations (August 2006). The EAA authorizes the Secretary of Commerce to regulate exports of commodities, software, and technology (collectively referred to as "items") based on national security and foreign policy objectives. Under the EAA, controls are placed on exports of items based on the technical capabilities of such items and also based on the destination of such exports. The EAA currently is lapsed, but the Export Administration Regulations remain in effect through the International Emergency Economic Powers Act (described below), Executive Order 13222, and the Presidential Notice of August 3, 2006.
- **Exon-Florio Amendment to the Defense Production Act and Executive Orders 11858, 12188, and 12661** (May 1975, January 1980, and December 1988). These provisions authorized the creation of the Committee on Foreign Investment in the United States (CFIUS), which is an interagency committee chaired by the Department of the Treasury. The mission of CFIUS is to review and potentially recommend that the President block foreign acquisitions of U.S. companies that threaten to impair national security.
- **International Emergency Economic Powers Act (IEEPA)** (October 1977). This act authorizes the President to engage in a wide variety of activities to deal with an unusual and extraordinary threat to the country's national security, foreign policy, or economy. To trigger authorities under IEEPA, the threat must originate in whole or substantial part from outside the United States, and the President must declare a national emergency with respect to such threat. Using IEEPA, the President has continued the Export Administration Regulation in effect despite the lapse of the EAA, as amended (see above).

National Strategies

- **The National Strategy for Homeland Security** (July 2002). The National Strategy for Homeland Security characterizes terrorism as any premeditated, unlawful act dangerous to human life or public welfare intended to intimidate or coerce civilian populations or governments. This description captures the core concepts shared by the various definitions of terrorism contained in the U.S. Code, each crafted to achieve a legal standard of specificity and clarity. This description covers kidnappings;

hijackings; shootings; conventional bombings; attacks involving chemical, biological, radiological, or nuclear weapons; cyber attacks; and any number of other forms of malicious violence. Terrorists can be U.S. citizens or foreigners, acting in concert with others, on their own, or on behalf of a hostile nation. Terrorists may seek to cause widespread disruption and damage, including casualties, by attacking our electronic and computer networks, which are linked to other critical infrastructures such as our energy, financial, and securities networks. Terrorist groups already are exploiting new information technology and the Internet to plan attacks, raise funds, spread propaganda, collect information, and communicate securely. As terrorists further develop their technical capabilities and become more familiar with potential targets, cyber attacks will become an increasingly significant threat. Accordingly, DHS will place an especially high priority on protecting our cyber infrastructure. Actions to reduce America's vulnerability to terrorism also must harness the coordinated effort of many Federal departments and agencies that have highly specialized expertise and long-standing relationships with industry.

- **The National Strategy to Secure Cyberspace** (July 2002). This strategy states that a top priority for the Nation is to understand infrastructure interdependencies and improve the physical security of cyber systems and telecommunications. The strategy directs DHS to work with State and local governments to establish strong IT security programs. It also describes the National Cyberspace Security Response System.
- **National Strategy for the Physical Protection of Critical Infrastructures and Key Assets** (February 2003). This national strategy puts forth strategic objectives to identify and assure the physical protection of critical infrastructure and assets; to provide timely warning and assure the protection of those infrastructures and assets that face a specific, imminent threat; and to assure the protection of infrastructures and assets that may become targets over time by pursuing specific initiatives and enabling a collaborative environment between the public and private sector.
- **National Counterintelligence Strategy** (March 2005). This strategy seeks to ensure that industry is not disadvantaged by foreign intelligence operations and provides appropriate threat information to industry and IT security partners to take appropriate risk mitigation measures. The strategy recognizes that the U.S. strategic response to today's threats require that the Nation's counterintelligence capabilities need to address technical, cyber, and human threats.

Management and Acquisition of Federal Government Information Technology

- **Clinger-Cohen Act of 1996** (AKA Information Technology Management Reform Act) (February 1996). Recognizing the importance of IT for effective government, Congress and the President enacted the Information Technology Management Reform Act and the Federal Acquisition Reform Act. These two acts, together known as the Clinger-Cohen Act, require the heads of Federal agencies to link IT investments to agency accomplishments. The Clinger- Cohen Act also requires that agency heads establish a process to select, manage, and control their IT investments. This act also reformed the way the Federal Government acquires and manages IT through performance-based and results-based management. The law focuses on IT investment management, information resources management, and IT management. It also directs all Federal agencies to use a formal enterprise architecture process. It transferred IT responsibilities from the General Services Administration (GSA) to OMB and further defined the role of an agency's CIO.
- **Executive Order (EO) 13011, Federal Information Technology** (January 2003). This EO outlines a coordinated IT approach that builds on current structures and successful practices to improve Federal Government mission performance and service delivery. Establishes the CIO Council, Government Information Technology Services Board, and Information Technology Resources Board to advise the President in carrying out the responsibilities of the Clinger-Cohen Act.
- **Memorandum to Heads of Selected Departments and Agencies, Interagency Support for Information Technology** (March 1997). This memorandum institutes funds for carrying out EO 13011.

- **Federal Acquisition Regulation, Part 39, Acquisition of Information Technology** (February 2006). This regulation establishes acquisition policies and procedures for acquiring information and IT (excluding national security systems).
- **E-Government Act of 2002** (January 2002). This act improves electronic Federal Government processes and services promotion and management through the establishment of a Federal CIO at OMB. The act establishes a measurement framework that requires using Internet-based IT to help citizens gain better access to services and information.
- **The Paperwork Reduction Act of 1995** (May 1995). This act establishes that the OMB Director will develop and oversee the "implementation of policies, principles, standards, and guidelines for information technology functions and activities of the Federal Government" to help enhance agency mission performance.
- **Federal Information Security Management Act** (FISMA) of 2002 (November 2002). This act establishes a framework for the security of the Federal Government's IT by mandating annual audits of Federal Government entities and those organizations affiliated with the Federal Government.

Information Technology Audit-Related Authorities

- **Health Insurance Portability and Accountability Act (HIPAA)** (August 1996). Seeks to enhance health insurance coverage portability and continuity; stop health insurance and health care delivery waste, fraud, and abuse; foster medical savings accounts; increase long-term care services and coverage access; and make health insurance administration less complicated. The HIPAA Security Rule establishes minimum standards that safeguard electronic protected health information.
- **Gramm-Leach-Bliley Act (GLBA)** (September 1999). This act establishes the way in which personal information about individuals who obtain financial products or services from financial institutions is shared. Three rules manage personally identifiable information: (1) a financial institution is required to provide a customer with a privacy notice; (2) every financial institution is to create an information security plan; and (3) financial institutions must take precautions to prevent pretexting (i.e., obtaining personally identifiable information without proper authority).
- **Sarbanes-Oxley Act (SOX) of 2002** (July 2002). This act establishes policies related to corporate governance, the practice of public accounting, and financial disclosure. Section 404 largely affects every company's IT department as it outlines processes for addressing such things as installation of new business applications, application monitoring, and IT system and network security.
- **Foreign Corrupt Practices Act (FCPA) of 1977** (15 United States Code (U.S.C.) 78dd-1, et seq.) (November 1988). The FCPA seeks to thwart corporate bribery of foreign officials by requiring companies to maintain accurate books, records, and accounts and by requiring publicly traded companies to retain internal accounting control systems.
- **The Cyber Security Enhancement Act of 2002** (February 2002). The Cyber Security Enhancement Act of 2002 amends Federal computer crime sentencing guidelines, making it possible to issue more appropriate sentences for crimes involving fraud in connection with computers and access to protected information, protected computers, restricted data in interstate or foreign commerce, or involving a computer used by or for the Federal Government.
- **The Computer Fraud and Abuse Act of 1984 as amended by the Computer Abuse Amendments Act of 1994** (September 1994). Note: Section 1030 was amended on October 26, 2001, by the USA PATRIOT antiterrorism legislation. Section 1030: Fraud and related activity in connection with computers states that whoever, having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the U.S. Government pursuant to an executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y of Section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the

United States, or to the advantage of any foreign nation, willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it.

National Preparedness and Response Authorities Related to Information Technology

- **Executive Order (EO) 12656, Assignment of Emergency Preparedness Responsibilities** (November 1988). This EO delegates national security and emergency preparedness (NS/EP) responsibilities to Federal departments and agencies and instructs agencies to create plans and capabilities that will ensure continuity of essential operations.
- **Defense Production Act of 1950, as amended (DPA)** (June 1998). This act authorizes the President to, among other things, demand that companies accept and give priority to Federal Government contracts that the President "deems necessary or appropriate to promote the national defense." In 2003, the DPA was amended, so that the term "national defense" includes "critical infrastructure protection and restoration." The act authorizes the provision of financial incentives for certain technological development and domestic production.
- **National Response Plan** (December 2004). Emergency Support Function (ESF) #2, Communications, coordinates Federal actions to support temporary NS/EP telecommunications and telecommunications infrastructure restoration. During response efforts, ESF#2 supports all Federal departments and agencies in the procurement and coordination of all NS/EP telecommunications services from the telecommunications and IT industry. The Cyber Security Incident Annex outlines policies, responsibilities, organization, and actions so that the Nation can prepare for, respond to, and recover from nationally significant events related to cyber.
- **The Robert T. Stafford Disaster Relief and Emergency Assistance (Stafford) Act** (October 2000). The Stafford Act gives the President authority to declare a major disaster so Federal resources can be mobilized and distributed to provide relief to the affected States. Assistance is authorized for preparedness, emergency response, and recovery efforts, which involve the IT sector.

Information Technology Communications Related Authorities

- **Communications Act of 1934** (June 1934). This act regulates interstate and foreign wire or radio communication and established the Federal Communications Commission.
- **Telecommunications Act of 1996** (January 1996). Title V of the Telecommunications Act, entitled The Communications Decency Act of 1996, criminalizes the intentional electronic transmission of any communications that is obscene or indecent and prohibits the use of a computer network for the purpose of annoying or harassing recipients of messages.
- **Communications Assistance for Law Enforcement Act (CALEA)** (October 1994). CALEA, as it relates to IT, further defines the existing statutory obligation of telecommunications carriers to assist law enforcement in executing electronic surveillance of communications, such as VoIP and electronic messaging, pursuant to court order or other lawful authorization. The objective of CALEA implementation is to preserve law enforcement's ability to conduct lawfully authorized electronic surveillance while preserving public safety, the public's right to privacy, and the telecommunications industry's competitiveness.

Information Technology Privacy Authorities and Information Protection Related Authorities

- **Electronic Communications Privacy Act (ECPA)** (October 1986). This act establishes policies for access, interception, use, disclosure, and privacy protection of electronic communications for wire and electronic communications. ECPA prevents the Federal Government from mandating electronic communications disclosure without appropriate procedure.

- **The National Infrastructure Protection Act** (October 1996). This act defines "protected information" as "information that has been determined by the U.S. Government pursuant to an EO or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph (y) of Section 11 of the Atomic Energy Act of 1954." The National Infrastructure Protection Act changes the original language of 18 U.S.C. 1030, redefining computer crime from simply stealing information from a Federal computer system to include willfully harming the integrity and availability of the information or information system. The legislation acknowledges the fact that harm can come to information or information systems, not only through disclosure but also in the loss of the availability or integrity of the information that a system contains.

International Standards and Guidelines

- **International Organization for Standardization (ISO) 17799** (June 2005). ISO 17799 is a worldwide technical standard prepared by the British Standards Institution that is widely accepted as one of the definitive standards for information security. It is intended to serve as a single reference point for identifying a range of controls needed for situations where information systems are used in industry and commerce.
- **Organisation for Economic Co-operation and Development (OECD) Guidelines for the Security of Information Systems.** OECD guidelines are intended to raise awareness of risks to information systems and of the safeguards available to meet those risks. Their purpose is to create a general framework to assist individuals in the public and private sectors responsible for the development and implementation of coherent measures, practices, and procedures for the security of information systems; to promote cooperation between the public and private sectors in the development and implementation of such measures, practices, and procedures; to foster confidence in information systems and the manner in which they are provided and used; to facilitate development and use of information systems, nationally and internationally; and to promote international cooperation in achieving security of information systems.

Appendix 3: Common Risk Management Frameworks

Framework	Description
COBIT 3.0/4.0	The IT Governance Institute's (ITGI) COBIT provides a framework for supporting IT governance to assist organizations in ensuring that IT is aligned with the mission of the business, IT enables the business and maximizes benefits, IT resources are used responsibly, and IT risks are managed appropriately (ITGI, 2005).
Disaster Recovery Institute International (DRII)	Provides courses and training on disaster recovery, including activities and programs designed to return an entity to an acceptable condition and the ability to respond to an interruption in services by implementing a disaster recovery plan to restore an organization's critical business functions. (DRII 2004).
ISO 27001	An information security standard published in 2005 by the International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) entitled Information Technology—Security Techniques—Information Security Management Systems—Requirements. This standard provides requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented Information Security Management System (ISMS).
ISO/IEC 13335	The ISO/IEC guidance on the management of Information and Communication Technology (ICT) security. Part 1 of ISO/IEC 13335 presents the concepts and models fundamental to a basic understanding of ICT security and addresses the general management issues that are essential to the successful planning, implementation, and operation of ICT security. The other parts provide operational guidance on ICT security. Together, these parts can be used to help identify and manage all aspects of ICT security.
ISO/IEC 17799	An information security standard published in 2005 by the ISO/IEC entitled Information Technology—Security Techniques—Code of Practice for Information Security Management. This standard provides best practice recommendations on information security management for use by those who are responsible for initiating, implementing, or maintaining information security management systems.
ISO/IEC 21827	The SSE-CMM®, a process reference model, is focused on the requirements for implementing security in a system or series of related systems that are the ITS domain. Within the ITS domain, the SSE-CMM model is focused on the processes used to achieve ITS—specifically on the maturity of those processes. There is no intent within the SSE-CMM model to dictate a specific process to be used by an organization, let alone a specific methodology.
ITIL Security Management	The United Kingdom's Office of Government Commerce (OCG) ITIL Security Management provides a framework for assisting organizations in ensuring that security controls are implemented and maintained to address changing circumstances, such as changed business and IT service requirements, IT architecture elements, and threat; that security Incidents are managed; that audit results show the adequacy of security controls and measures taken; and that reports are produced to show the status of information security (OCG 2005).

Framework	Description
NIST Special Publication 800-12	The *NIST Handbook* provides a broad overview of computer security to help readers understand their computer security needs and develop a sound approach to the selection of appropriate security controls. It provides assistance in securing computer-based resources (e.g., hardware, software, and information) by explaining important concepts, cost considerations, and interrelationships of security controls. (NIST 2004).
NIST Special Publication 800-30	The *NIST Risk Management Guide for Information Technology Systems* provides a framework for developing effective risk management programs within organizations. This guide defines risk management as the process of identifying risk, assessing risk, and taking steps to reducing risk to an acceptable level (NIST 2002).
NIST Special Publication 800-53	The *NIST Recommended Security Controls for Federal Information Systems* provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the Federal Government. These guidelines apply to all components of an information system that process, store, or transmit Federal information (NIST 2005).
OCTAVE	OCTAVE is a self-directed information security risk assessment process developed by Carnegie Mellon University and sponsored by DOD. The main objective of this standard is to assist organizations in improving their ability to manage information security risks and protect themselves from cyber threats (Software Engineering Institute, Carnegie Mellon University, 2001).

Appendix 4: IT Sector-Related Protective Programs

Table A4-1 presents brief descriptions of some of the existing protective programs (primarily Federal) that support the overarching IT Sector goals. Numerous other protective programs across the private sector; Federal, State, regional, local, and tribal government; and other organizations also enhance the physical, cyber, and human security of the sector.

Table A4-1: Existing Protective Programs that Support the Overarching IT Sector Goals

Protection/Prevention	
Protective Program	**Program Description**
Vulnerability Reduction	
Common Vulnerabilities and Exposures (CVE)	A mechanism for standardizing names for vulnerabilities and other information security exposures.
DHS Control Systems Security Initiative	DHS sponsors programs to increase the security of control systems.[38] 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 CI/KR sectors.
DHS Strategic Homeland Infrastructure Risk Assessment (SHIRA)	SHIRA is designed to represent the status of vulnerability in the Nation's infrastructure.
NIST National Vulnerability Database (NVD)	NVD is a comprehensive cyber security vulnerability database that integrates all publicly available U.S. Government vulnerability resources and provides references to industry resources. It is based on the CVE vulnerability naming standard.
US-CERT Malicious Code Analysis Program	This program includes: (1) a laboratory for analyzing malicious code and developing countermeasures, and (2) a CVE dictionary system to correlate information across vendor products.
Threat Assessment	
DHS HITRAC	HITRAC conducts integrated threat analysis for CI/KR within the DHS. HITRAC brings together intelligence and infrastructure specialists to ensure a complete and sophisticated understanding of the risks to U.S. CI/KR, including cyber infrastructure.

[38] A control system is an interconnection of components (designed to maintain operation of a process or system) 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 CI/KR and may be vulnerable to increasing cyber threats that could have a devastating impact on national security, economic security, public health and safety, and the environment.

Protection/Prevention	
Protective Program	**Program Description**
DOJ Computer Crimes and Intellectual Property Section (CCIPS)	DOJ's CCIPS is responsible for prosecuting nationally significant cases of cyber crime and intellectual property crime. In addition to its direct litigation responsibilities, the section formulates and implements criminal enforcement policy and provides advice and assistance.
FBI Cyber Crimes Division	The cyber mission is fourfold: (1) stop those behind the most serious computer intrusions and the spread of malicious code; (2) identify and thwart online sexual predators who use the Internet to meet and exploit children and to produce, share, or possess child pornography; (3) counteract operations that target U.S. intellectual property, endangering our national security and competitiveness; and (4) dismantle national and transnational organized criminal enterprises engaging in Internet fraud.
National Counterintelligence Center (NCIX)	NCIX, which serves as head of national counterintelligence for the U.S. Government, is directly responsible to the Director of National Intelligence. The NCIX facilitates and enhances U.S. counterintelligence (CI) efforts and awareness by: (1) enabling the CI community to better identify, assess, prioritize, and counter intelligence threats from foreign powers, terrorist groups, and other non-state entities; (2) ensuring the CI community acts efficiently and effectively; and (3) providing for the integration of all U.S. counterintelligence activities.
Community Acquisition Risk Center (CARC)	CARC performs threat analysis and risk methods/tools for Federal agencies. Also performs a threat analysis of foreign commercial entities that seek commercial relations with U.S. intelligence agencies.
US-CERT	US-CERT, established in 2003 to protect the Nation's Internet infrastructure, coordinates defense against and responses to cyber attacks across the Nation. US-CERT collaborates with Federal agencies, the private sector, the research community, State and local governments, and international entities. By analyzing incidents reported by these entities and coordinating with national security incident response centers responding to incidents on classified and unclassified systems, US-CERT disseminates actionable cyber security information to the public. US-CERT carries out numerous activities: Maintains 24/7 Secure Operations Center; Acts as a trusted third-party to assist in the responsible disclosure of vulnerabilities; Develops and participates in regional, national, and international level exercises; Supports forensic investigations with recursive analysis on artifacts; Provides malicious software (malware) analytic and recovery support for government agencies; Provides behavior techniques for dynamic and static analysis; Manages the malicious code submission and collection program; Disseminates emerging cyber threat warnings; Administers the National Cyber Alert System to disseminate cyber security information to all Americans; Provides fused current and predictive cyber analysis based on situational reporting; Provides on-site incident response capabilities to Federal and State government departments and agencies; Supports ongoing Federal law enforcement investigations; Coordinates Federal programs of computer emergency response team and Chief Information Security Officer peer groups for sharing incident information, best practices, and other cyber security information; and Collaborates with domestic and international computer security incident response teams.

Protection/Prevention	
Protective Program	**Program Description**
United States Secret Service (USSS) Electronic Crimes Task Force (ECTF)	ECTFs provide interagency coordination on cyber-based attacks and intrusions. At present, 15 ECTFs are in operation, with an expansion planned.
USSS National Threat Assessment Center (NTAC)	NTAC was created to provide leadership and guidance to the emerging field of threat assessment. Specifically, NTAC offers timely, realistic, useful, and effective advice to law enforcement and other professionals and organizations with responsibilities to investigate and/or prevent targeted violence.
Modeling and Simulation	
NCS/National Coordinating Center for Telecommunications / Network Design and Analysis Center (NDAC)	NDAC is a modeling and analysis tool designed to view the public switched network (PSN) (including the public switched telephone network (PSTN), Internet Protocol (IP), next generation packet networks, and wireless and satellite infrastructures) under various stress conditions. NDAC software resources include the tools, models, and telecommunications databases used to assess network performance, perform modeling and simulation, and visualize network topologies.
National Infrastructure Simulation and Analysis Center (NISAC)	NISAC is a joint program with Sandia National Laboratories that provides modeling, simulation, and analysis of critical infrastructures, their interdependencies, complexities, and the potential consequences of disruptions.
High Assurance Products and Services Programs	
Air Force Research Laboratory Anti-Tamper—Software Protection Initiative (AT-SPI)	The AT-SPI Technology Office is charged with developing technologies to prevent/delay the exploitation of critical program information. Of particular concern is the need to protect critical design elements or manufacturing processes. Anti-tamper technology development efforts must balance the need to protect critical technologies from exploitation, with the need to minimize the impact of anti-tamper technology application on system performance, operations and maintenance, and cost.
DHS Software Assurance Program	The DHS is leading a Software Assurance Program that addresses processes, technology, and acquisition throughout the software life cycle to result in secure and reliable software that supports critical mission requirements.

Protection/Prevention	
Protective Program	**Program Description**
NSA Information Assurance Directorate (IAD) Capabilities Presentations Commercial Off-the-Shelf (COTS) Product Evaluations Communications Security Evaluation Programs Controlled Cryptographic Item Agreement Global Information Grid Independent Research and Development Program IA Courseware Evaluation Program IA Outreach Information Systems Security INFOSEC Assurance Training and Rating Program National Information Assurance Partnership (NIAP)	NSA's IAD is dedicated to providing information assurance solutions that will keep our information systems safe. IAD's mission involves detecting, reporting, and responding to cyber threats; making encryption codes to pass information securely between systems; and embedding information assurance (IA) measures directly into the emerging Global Information Grid. NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) for IT security. CCEVS is a partnership between the public and private sectors. This program is being implemented to help consumers select COTS IT products that meet their security requirements and to help manufacturers of those products gain acceptance in the global marketplace.

Situational Awareness	
Protective Program	**Program Description**
Tactical Indications, Analysis, and Warning	
DHS Common Operating Picture (COP)/Common Operating Database (COD)	The DHS is currently developing a COP system, a situational awareness application for crises to facilitate effective information sharing and decisionmaking, and rapid staff actions. The COP is a display of relevant information that is derived from a COD and is shared by multiple agencies and organizations. Accessible through HSIN, the COP/COD system will provide a common operating database for interagency crises information sharing to ensure a common understanding of the situation and facilitate timely, risk-mitigated decisionmaking. The COP/COD system is a Web-served mission application that does not require participants to install any additional hardware or software. The DHS components and interagency partners will access the COP/COD through the HSIN; leverage the shared interagency operational database, and integrate functional and analytical tools into their operations as needed. The COP/COD system includes functional screens that address national and international situation summaries, executive actions, RFIs, blue force status, chronology, critical infrastructure, geospatial representations specified by the user, media monitoring products, video products from the field, functional metrics, and HSIN information linkages. Currently, the COP/COD development efforts have focused on preparing for the 2006 hurricane season and implementation in the selected DHS offices, and component and interagency operation centers. Subsequently, the COP/COD system will be implemented in the additional DHS component and interagency operation centers and will serve as a key information-sharing tool during crisis situations.

Situational Awareness	
Protective Program	**Program Description**
FBI/DHS Cyber Incident Detection Data Analysis Center (CIDDAC)	CIDDAC provides voluntary automated incident reporting to law enforcement when security breaches occur, while protecting the identity and privacy of its members and their data. CIDDAC is a nonprofit organization that integrates private, public, and government cooperation to facilitate the real-time sharing of cyber attack data.
International Watch and Warning Network (IWWN)	The IWWN consists of cyber security policy, computer emergency response, and law enforcement participants from 15 countries. The IWWN will provide a mechanism for participating countries to share information to build global cyber situational awareness and coordinate incident response.
US-CERT Einstein Program	Program is designed to build cyber-related situational awareness. It provides an automated process for collecting, correlating, analyzing, and sharing computer security information across the Federal civilian government. This automated system facilitates flow data sharing from Federal Government agencies' Internet access gateways and analyzes associated traffic patterns and behavior and provides US-CERT and participating agencies a better cyber security view and understanding across the Federal Government.
US-CERT National Cyber Alert System	US-CERT National Cyber Alert System delivers targeted, timely, and actionable information to all citizens—computer security professionals to home computer users with basic skills—to allow them to secure their computer systems. The system identifies, analyzes, and prioritizes emerging vulnerabilities and threats. It relays computer security update and warning information to all users. Alerts are issued to subscription mailing lists as well as posted on the US-CERT Web site (www.uscert.gov).
Information Sharing / Communications Mechanisms	
FBI InfraGard	InfraGard provides a trusted forum for the exchange of knowledge, experience, and information related to the protection of our Nation's critical infrastructure from physical and cyber threats. InfraGard provides its members with unmatched opportunities to promote the physical and cyber security of their organizations through access to a trusted, national network of Subject Matter Experts (SME) from the public and private sectors, spanning from the corporate and Federal to the local level. The program further provides government stakeholders, across the Federal, State, and local levels, with access to the expertise and experience of critical infrastructure owners and operators. The more than 17,000 InfraGard SMEs are active in all 50 States and represent a cross section of critical infrastructures. InfraGard members can bring subject matter expertise to the public and private sectors by State, region, or city.
Government and NSTAC Network Security Information Exchanges (NSIE)	NSIE representatives voluntarily share information related to threats, incidents, and vulnerabilities affecting operations, administration, maintenance, and provisioning systems supporting the telecommunications infrastructure. This information includes attempted or actual penetrations or manipulations of software, databases, and systems related to critical NS/EP telecommunications. In addition, representatives share information on physical intrusions pursuant to electronic attacks on network assets.

Situational Awareness	
Protective Program	**Program Description**
HSIN	HSIN is a national, Web-based communications platform that enables the DHS; the SSAs; State, local, and tribal government entities; and other security 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 NIPP-related steady-state CI/KR protection and NRP-related incident management activities. The network also will provide information-sharing processes that form the bridge between these two homeland security missions. HSIN will be one part of the ISE called for by the Intelligence Reform and Terrorism Prevention Act of 2004; as specified in the act, HSIN will provide users with access to terrorism information that is matched to their roles, responsibilities, and missions in a timely and responsive manner. HSIN-CS is a secure, unclassified, Web-based communications system that serves as the DHS's primary nationwide information-sharing and collaboration network. HSIN-CS offers real-time chat and instant messaging capability, as well as a document library that contains reports from multiple Federal, State, and local sources. It supplies information on suspicious incidents and pre-incidents, mapping and imagery tools, 24/7 situational awareness, and analysis of terrorist threats, tactics, and weapons. HSIN provides connectivity between NOC, critical private industry, and Federal, State, and local organizations responsible for or involved in combating terrorism, responding to critical incidents, and managing special events.
IT-ISAC	IT-ISAC alerts are part of the early warning system for cyber attacks; many of the companies whose products are the foundation of the Nation's IT infrastructure are members of the IT industry ISAC. Coordinates information sharing on cyber vulnerabilities among IT companies and the U.S. Government.
MS-ISAC	The mission of the MS-ISAC is to provide a common mechanism for raising the level of cyber security readiness and response in each State and with local governments. The MS-ISAC provides a central resource for gathering information on cyber threats to critical infrastructure from the States and provides two-way sharing of information between and among State and local government.
Regional Information Sharing Systems® (RISS)	RISS is a federally funded program administered by DOJ, Office of Justice Programs, and Bureau of Justice Assistance. RISS serves more than 7,300 member law enforcement agencies in 50 States, Canada, the District of Columbia, Australia, Guam, the U.S. Virgin Islands, England, and Puerto Rico. The program consists of 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. A majority of 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; USSS; 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.

Situational Awareness	
Protective Program	**Program Description**
US-CERT Portal	The US-CERT Portal is a secure, Web-based collaborative system that enables members to communicate and collaborate on a real-time, 24/7 basis about emerging cyber threats and vulnerabilities. Through a suite of tools such as secure messaging, forms, secure chat rooms, alerts, and shared libraries, US-CERT is able to disseminate information to targeted audiences. As an incident reporting mechanism, it serves as a central repository of Federal incident data, ensuring that incident reports will be cataloged, indexed, and prioritized for analysis. The portal also contains four forums on emerging threats, malware code analysis, incident response, and vulnerabilities that portal members can use to collaborate on a real-time basis as necessary. The forums provide an opportunity for members to discuss suspicious activity, ask for advice, post news articles, and discuss topics of interest with other members. Forums can be tailored to a specific audience or can be created so that access is granted to everyone.

Response, Recovery, and Reconstitution	
Protective Program	**Program Description**
National Emergency Communications	
CWIN	CWIN is a government network within HSIN that provides mission-critical connectivity and a survivable DHS capability for information sharing, collaboration, and alerting among Federal, State, and local agencies for critical infrastructure restoration when primary forms of communication are unavailable. CWIN is a communication network designed to facilitate information sharing and collaboration of critical infrastructure and cyber information, and issue immediate alerts and notifications. CWIN communities of interest include: (1) entities in the private sector vital to restoring the Nation's critical infrastructures (e.g., electrical, IT, and telecommunication, (2) entities in the Federal and State government vital to maintain government-wide connectivity with the DHS, (3) sector-specific agencies and resources, (4) State homeland security advisors, (5) emergency management centers, and (6) international partners.
Telecommunications Service Priority (TSP)	TSP provides the regulatory, administrative, and operational framework for priority restoration and provisioning of NS/EP communications circuits in the event of an emergency. Eligibility in the TSP Program extends to Federal, State, and local government, private industry, or foreign governments that have communications services supporting an NS/EP mission.
WPS	WPS provides priority commercial mobile radio service during and after emergencies for NS/EP personnel by ensuring WPS calls receive the next available radio channel during times of wireless congestion. WPS helps to ensure that key NS/EP personnel can complete critical calls by providing priority access during times of wireless network congestion to key leaders and supporting first responders. In conjunction with GETS, it provides an end-to-end solution.
GETS	GETS provides emergency access and priority processing in the local and long distance segments of the Public Switched Telephone Network (PSTN), increasing the likelihood that NS/EP personnel can complete critical calls during periods of PSTN congestion resulting from natural or manmade disasters. GETS supports Federal, State, and local government, industry, and nonprofit organization personnel in performing their NS/EP missions. GETS uses three major types of networks: major long distance networks, local networks, and government-leased networks.

Response, Recovery, and Reconstitution	
Protective Program	**Program Description**
Incident Management / Response Coordination	
DOD Cyber Crime Center (DC3)	DC3 was created to better address the proliferation of computer crimes within or directed at DOD. The DC3 has three main programs: DOD Computer Forensics Laboratory (DCFL), DOD Computer Investigations Training Program (DCITP), and DOD Cyber Crime Institute (DCCI).
HSOC	HSOC serves as the Nation's hub for information sharing, situational awareness, and domestic incident management. HSOC increases coordination among Federal, State, local, tribal, and private sector partners, as well as select members of the international community. Capabilities include information collection and analysis; situational awareness and incident response coordination; and development and dissemination of threat warning products.
The Internet Fraud Complaint Center (IFCC)	The IFCC's mission is to address fraud committed over the Internet. It provides a convenient, easy-to-use reporting mechanism that alerts authorities of a suspected criminal or civil violation. It also offers a central repository for complaints related to Internet fraud.
National Cyberspace Security Response System/Program Government Forum of Incident Response and Security Teams (GFIRST) Internet Disruption Working Group (IDWG) NCRCG US-CERT: North American Incident Response Group	GFIRST, established by the DHS, facilitates interagency information sharing and cooperation across Federal agencies responsible for cyber system readiness and response. Members work together to understand and manage computer security incidents, and encourage proactive and preventive security practices. The IDWG, which was established by the DHS in January 2005, is a strategic partnership to assist the NCRCG, the US-CERT, and the private sector to coordinate contingency plans for recovering Internet functions in the event of a cyber-related incident. This working group collaborates with major security partners to identify and prioritize the short-term protective measures necessary to prevent major disruptions of the Internet or reduce their consequences, and to identify responsive/reconstitution measures for contingency plans in the event of a major disruption. 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"). 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. US-CERT: North American Incident Response Group (includes US-CERT, computer security incident response teams, ISACs, managed security providers, vendors, security providers, and others).
NICC	NICC is a 24/7 watch operation center that maintains operational and situational awareness of the Nation's CI/KR sectors. NICC provides a centralized mechanism and process for information sharing and coordination between and among government, SCCs, GCCs, and other industry partners. Capabilities include the following: *Alerts and Warnings*—threat-related information products to industry partners; and *Reporting*—suspicious activity and potential threats.

Response, Recovery, and Reconstitution	
Protective Program	**Program Description**
US-CERT Cyber Forensics Training Program (with the Computer Emergency Response Team Coordination Center) and Law Enforcement) Cybercop Portal	The Cybercop Portal is a private sector initiative that is sponsored by government and industry. It is a secure Internet-based information-sharing mechanism that connects more than 8,700 members of the law enforcement community worldwide (e.g., bank investigators and the network security community) involved in electronic crimes investigations.
Contingency Planning / National Level Planning	
National Cyber Exercises	The DHS conducts exercises to identify, test, and improve coordination of the cyber incident response community, including Federal, State, Territorial, local, tribal, and international government elements, as well as private sector corporations and coordinating councils.
Top Officials (TOPOFF) Exercises	TOPOFF is a 2-year cycle of seminars, planning events, and exercises designed to strengthen the Nation's capacity to prevent, prepare for, respond to, and recover from terrorist attacks involving Weapons of Mass Destruction (WMDs). The DHS Office for State and Local Government Coordination and Preparedness (SLGCP) sponsors the TOPOFF series.
Reconstitution Plans and Programs	
NetGuard	NetGuard is a DHS-led initiative that will bring together the public sector with the State and local community following an incident that affects information systems and communications networks. The intent of the initiative is to create teams of volunteers from the private sector that could provide technical assistance and resources to the affected community. The program also could act as a clearinghouse for matching the needs of the local government and businesses with available resources in a timely manner.
Web Emergency Operations Center (WebEOC)	WebEOC is a Web-based emergency management communications system that provides cost-effective, real-time information sharing. By linking national, State, local, and even international sources, WebEOC helps to facilitate decisionmaking in emergency situations.

Appendix 5: Action Items

Section 1

Near Term (~1 year)

- Facilitate the development of and articulate for IT Sector members the national security and business value for participation in SSP implementation activities. (*NCSD, SCC, and GCC*)
- Develop criteria that may be used for determining nationally significant events. (*NCSD, SCC, GCC, and NCRCG*) (*Underway*)
- Provide input into national-level efforts to clarify the roles and responsibilities of public and private sectors in Federally coordinated response, recovery, and reconstitution efforts involving nationally significant events. (*NCSD, SCC, GCC, and NCRCG*)
- Provide public and private sector perspectives and input to assist in planning for Federally coordinated response and recovery efforts involving nationally significant events. (*NCSD, SCC, GCC, and NCRCG input*)

Long Term (1-3 years)

- Conduct exercises that test the implications of a nationally significant event and the resulting public and private sector roles, responsibilities, and capabilities. (*NCSD, SCC, GCC and NCRCG*)
- Annually review and revise IT SSP goals, objectives, and authorities. (*GCC and SCC*)
- Hold joint IT and Communications Sector meetings biannually to address issues of interest to both sectors, and discuss potential areas for collaboration. (*NCSD, NCS, SCC, GCC, Communications SCC, Communications GCC*)
- Work in partnership through the PCIS with the Communications Sector to help other CI/KR understand their dependence on the IT and Communications Sectors. (*NCSD, NCS, SCC, GCC, Communications SCC, Communications GCC*)

Section 2

Near Term (~1 year)

Actions to develop the IT Sector Risk Profile:

- Develop an implementation plan for the 2007 IT Sector Risk Profile. (*NCSD with GCC and SCC input*)
- Identify resources needed to implement the 2007 IT Sector Risk Profile. (*NCSD with GCC and SCC input*)

- Select the appropriate entity to manage and protect IT Sector risk management information. (*SCC, IT-ISAC, and GCC*)
- Decompose the sector's critical functions and/or sub-functions. (*SCC, IT-ISAC, and GCC*)
- Develop initial draft measurements and thresholds for consistently evaluating consequences, vulnerabilities, and threats to enable comparable risk assessment results. (*SCC and IT-ISAC with GCC input*)
- Initiate the identification of the sector's nationally consequential threats, and conduct analysis of them against the critical IT Sector functions. (*GCC, IT-ISAC, HITRAC, and IC*)
- Initiate the identification and assessment of vulnerabilities and consequences for critical IT Sector functions. (*IT-ISAC with GCC input*)
- Initiate the identification and assessment of mitigations that address threat, vulnerability, and/or consequences. (*IT-ISAC and GCC*)
- Collaborate with the Communications Sector regarding the identification and risk assessment of the Internet infrastructure, including specifically physical and cyber threat assessments for the Internet. (*SCC, IT-ISAC, and GCC*)

Other actions:

- Continue to encourage participation in the IT SCC and IT GCC. (*SCC, IT-ISAC, and GCC*)
- Encourage IT Sector entities to consider adopting individual risk management approach(es) appropriate for their unique operating environments. (*SCC and IT-ISAC*)
- Collaborate and coordinate with the other CI/KR sectors to address threats outside the IT Sector's control. (*SCC, IT-ISAC, and GCC*)

Long Term (1-3 years)

- Review (annually) critical IT Sector functions to determine if technological and environmental changes have occurred that alter the set of functions or their descriptions. (*SCC and GCC*)
- Identify (annually) threats, vulnerabilities, consequences, and mitigations that are of national significance to the sector. (*SCC, IT-ISAC, GCC, HITRAC, and IC*)
- Define and refine the IT Sector risk profile over time as the approach described in this section is implemented and repeated. (*GCC, SCC, HITRAC, and IC*)
- Improve cross-sector coordination. (*SCC, IT-ISAC, and GCC*)

Section 3

Near Term (~1 year)

- Establish the joint IT SCC and IT GCC Protective Program Working Group to review existing protective programs, identify private sector protective programs, and refine and consolidate the list of current programs. (*NCSD, SCC, and GCC*)
- Hold annual meeting on protective programs before developing the IT Sector CI/KR Protection Annual Report. (*NCSD, SCC, and GCC*)

Long Term (1-3 years)

- Raise awareness of elected and appointed officials in all branches of State government of the IT Sector's role in CI/KR protection. *(NCSD with SCC, GCC, and NASCIO input)*
- Report on protective program successes and lessons learned in the IT Sector CI/KR Protection Annual Report. *(NCSD with SCC and GCC input)*
- Conduct joint discussions with the Communications Sector on protective program effectiveness and requirements for new protective programs to avoid duplication of efforts. *(NCSD, SCC, GCC, NCS, Communications SCC, and Communications GCC)*
- Manage protective programs sponsored by the Federal Government in close partnership with the private sector. *(NCSD, GCC, and other Federal departments and agencies)*

Section 4

Near Term (~1 year)

Focal Points for Information Sharing

- Coordinate and integrate IT-ISAC and IT SCC efforts by offering recipient IT-ISAC membership to all IT SCC members and defining the roles and responsibilities of each organization to coordinate initiatives more effectively, assign accountability, and minimize duplicative efforts. *(IT-ISAC and SCC)*
- Increase the IT-ISAC's reach by augmenting current recruitment efforts by instituting a partnership program whereby ISAC membership is offered to representatives of IT trade associations and other IT-related organizations. *(IT-ISAC and SCC)*
- Identify and share POC lists to improve the ability to draw on the subject matter expertise available throughout the sector and to interact and coordinate with law enforcement for routine preparedness activities, as well as crisis situations requiring continuity of operations and continuity of government activities. *(SCC, IT-ISAC, GCC, NCSD)*
- Exchange information with the Communications SCC and coordinate on issues related to convergence of the IT and telecommunications infrastructures. Designating an IT SCC representative to serve on the Communications SCC and including a Communications SCC representative on the IT SCC Executive Committee will facilitate the exchange of information. *(SCC)*

Policies and Procedures for Sharing and Reporting Incidents

- Work with State and local governments to refine the security focus of SLFCs and clarify the relationship between SLFCs and the private sector, including clarifying how SLFCs relate to other information sharing mechanisms sponsored by DHS and how information flows between entities. *(DHS and NCSD with input from SCC and GCC)*
- Develop a Concept of Operations (CONOP) to formalize information sharing within the IT-ISAC's membership and between the IT-ISAC and external organizations, including US-CERT. *(IT-ISAC) (Underway)*
- Develop a Private Sector CONOP to guide US-CERT interaction with the private sector. *(US-CERT with input from the ISAC community and other private sector security partners) (Underway)*
- Develop MOUs to establish, where appropriate and necessary, formal information sharing agreements at the organizational level to better facilitate data exchange. *(Individual GCC and SCC entities or other security partners as appropriate)*

Procedures for Protecting and Disseminating Sensitive Proprietary Industry Information

- Raise awareness about the PCII Program among Federal, State, and local government and private sector participants and articulate the value that participants in the PCII Program can derive from submitting sensitive information. *(DHS PCII Program)*

- Assess the use of the PCII Program for submitting sensitive information, including risk management information, to the government. (*SCC, other private sector entities, GCC, and State and local governments*)

Access to Classified and SBU Government Information

- Identify private sector security partners with Federal Government issued security clearances that should receive government information, and provide their names and pertinent contact information to the DHS and other Federal departments and agencies (e.g., the IC-IRC) to facilitate more timely and extensive sharing of critical and actionable classified intelligence information with appropriately cleared individuals and organizations. (*SCC, IT-ISAC, and NCSD*)
- Identify mechanisms for private sector and State and local government officials who have security clearances to gain access to classified information pertinent to the IT Sector. (*DHS with input from NCSD and NASCIO*)

Mechanisms for Communicating and Disseminating Information

- Identify, update, and maintain appropriate private sector and State and local government POCs who should participate in emergency communication mechanisms such as CWIN, ENS, GETS, and WPS. (*NCSD and NCS with SCC, IT-ISAC, and NASCIO input*)
- Routinely test and exercise processes, procedures, emergency communications systems, and capabilities, document lessons learned, and make recommendations for improvement. (*NCS with NCSD, SCC, and GCC input*)
- Use the Homeland Security Information Network for Critical Sectors (HSIN-CS) as a mechanism for exchanging information with IT Sector private sector security partners. As information is made available, the IT-ISAC will pull it from HSIN-CS and push it to IT-ISAC members for their use. (*NCSD and other components of DHS, IT-ISAC*)
- Adopt a common format (e.g., ISAC Council template) for presenting information that is shared with the IT Sector private sector security partners. (*NCSD working with other components of the DHS*)
- Develop a strategy to leverage the Homeland Security Information Network (HSIN) to exchange IT Sector information with State and local governments. The strategy may consider duplicating or leveraging the IT-ISAC process of pulling information from HSIN-CS and pushing it to IT-ISAC members. (*NCSD and other components of the DHS with NASCIO input*)

Long Term (1-3 years)

Focal Points for Information Sharing

- Encourage public and private sector security partners to commit to participating in the NIPP partnership model, specifically the ISACs, including the IT-ISAC and MS-ISAC. (*DHS Office of Infrastructure Protection, NCSD, NCS, and other DHS components*)
- Address areas of convergence, such as those identified in the President's National Security Telecommunications Advisory Committee (NSTAC), *NSTAC Report to the President on the National Coordinating Center,*[38] including developing an approach for a long-term regional communications and IT coordinating capability that serves all regions of the Nation, convening a conference to focus on cyber issues, and exploring ideas for a multi-industry coordinating center. (*NCSD, NCS, GCC, SCC, Communications SCC, Communications GCC*)

Policies and Procedures for Sharing and Reporting Incidents

- Undertake an initiative to characterize and map the flow of information between and among security partners for all stages of preparedness activities. This initiative should include information on who shares what information, who receives the information, and what networks and systems are being used to disseminate and exchange the information. (*NCSD and other DHS components with input from SCC, IT-ISAC, and GCC*)

[38] President's National Security Telecommunications Advisory Committee (NSTAC), *NSTAC Report to the President on the National Coordinating Center,* May 10, 2006.

Procedures for Protecting and Disseminating Sensitive Proprietary Industry Information

- Develop the mechanisms and capabilities (e.g., access controls, user rights, and authentication) needed to assure the private sector that its data will be protected. (*NCSD and other DHS components with input from SCC, IT-ISAC, and GCC*)
- Familiarize government entities with IT-ISAC tiered information sharing mechanisms and capabilities. (*NCSD and IT-ISAC*)

Access to Classified and SBU Government Information

- Explore ways of clarifying the procedures for handling FOUO, SBU, LES, and other sensitive information. (*Homeland Security Council with input from NCSD, SCC, and GCC*)

Mechanisms for Communicating and Disseminating Information

- Design, develop, and implement a protected information sharing architecture as outlined in the NIPP. (*DHS Office of Infrastructure Protection, Information Sharing Environment*)
- Exercise processes and procedures (e.g., standard operating procedures and CONOPs) and communication mechanisms (e.g., HSIN-CS, GETS, CWIN, and WPS) and evaluate lessons learned to enhance information sharing from a cultural, organizational, and technological perspective. (*NCSD, NCS, DHS Office of Infrastructure Protection, SCC, GCC*)
- Achieving an enhanced information sharing framework requires commitment from public and private sector security partners. Participation in the IT SCC and IT GCC requires commitment not only on the part of individual members, but also on the part of the organizations employing them. Implementation of the above actions cannot be achieved without a core group of committed individuals from the public and private sectors. This core group of individuals and organizations may not necessarily be the same as those who were responsible for outlining the vision for an enhanced information sharing framework. Investment in resources and human capital is necessary for success.

Section 5

Near Term (~1 year)

- Establish an IT Sector R&D Working Group and identify opportunities for public and private sector security partners to collaborate on R&D priorities. (*NCSD, S&T Directorate, SCC, and GCC*)
- Brief R&D institutions listed above on the SSP to raise awareness of IT Sector R&D priorities, goals and objectives, and risk management approach. (*NCSD, S&T Directorate, SCC, GCC*)
- Coordinate with the Communications Sector on R&D CI/KR protection priorities that overlap or have inherent synergies. (*NCSD, SCC, GCC, NCS, Communications SCC, Communications GCC*)

Long Term (1-3 years)

- Plan and execute annual IT Sector R&D Workshop, and share results with R&D public and private sector security partners. (*SCC and GCC*)
- Develop a 5-year roadmap for IT Sector R&D priorities and resource needs. (*S&T Directorate and NCSD with input from SCC and GCC*)

Section 6

Near Term (~1 year)

- Update the IT SSP annually. (*GCC and SCC*)
- Develop (annually) the IT Sector CI/KR Protection Annual Report. (*NCSD with GCC and SCC input*)
- Identify necessary resources to implement the IT SSP risk management approach, protective programs, information sharing mechanisms, R&D initiatives, and performance measurement. (*NCSD, GCC, and SCC*)
- Engage with and develop public sector programs to support the implementation and maintenance of the IT SSP. (*NCSD*)
- Coordinate closely with the Communications Sector on the development of the next Communications SSP. (*GCC and SCC*)

Long Term (1-3 years)

- Develop and facilitate training and education initiatives necessary to implement the IT SSP successfully. (*NCSD, GCC, and SCC*)
- Collaborate with the Communications Sector on outreach and education to customers on their reliance on Communications and IT infrastructures and security roles and responsibilities. (*NCSD, GCC, SCC, NCS, Communications SCC, Communications GCC*)
- Fulfill the roles and responsibilities identified in section 6.3. (*All*)

Section 7

Near Term (~1 year)

- Prioritize sector action items, taking into consideration available resources. (*NCSD, SCC, GCC*)
- Create Gantt chart for the sector that maps SSP actions to objectives and goals. (*NCSD with input from SCC and GCC*)

Long Term (1-3 years)

- Continue to reassess action item prioritization based on evolving status of the sector and resource availability. (*NCSD, SCC, and GCC*)
- Track sector action item progress and update the IT SSP. (*NCSD, SCC, and GCC*)

Homeland Security