Critical Infrastructure Partnership Advisory Council Annual

2008

Homeland Security

2008 Critical Infrastructure Partnership Advisory Council Annual

Contents

Overview

Cross-Sector Partnerships

- Partnership for Critical Infrastructure Security
- Federal Senior Leadership Council
- State, Local, Tribal, and Territorial Government Coordinating Council
- Regional Consortium Coordinating Council

Sector Partnerships

- Banking and Finance Sector
- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- National Monuments and Icons Sector
- Nuclear Sector
- Postal and Shipping Sector
- Transportation Sector
- Water Sector

Overview

"The CIPAC directly supports the sector partnership model by providing a legal framework for members of the SCCs and GCCs to engage in joint CIKR protection-related activities."

National Infrastructure Protection Plan

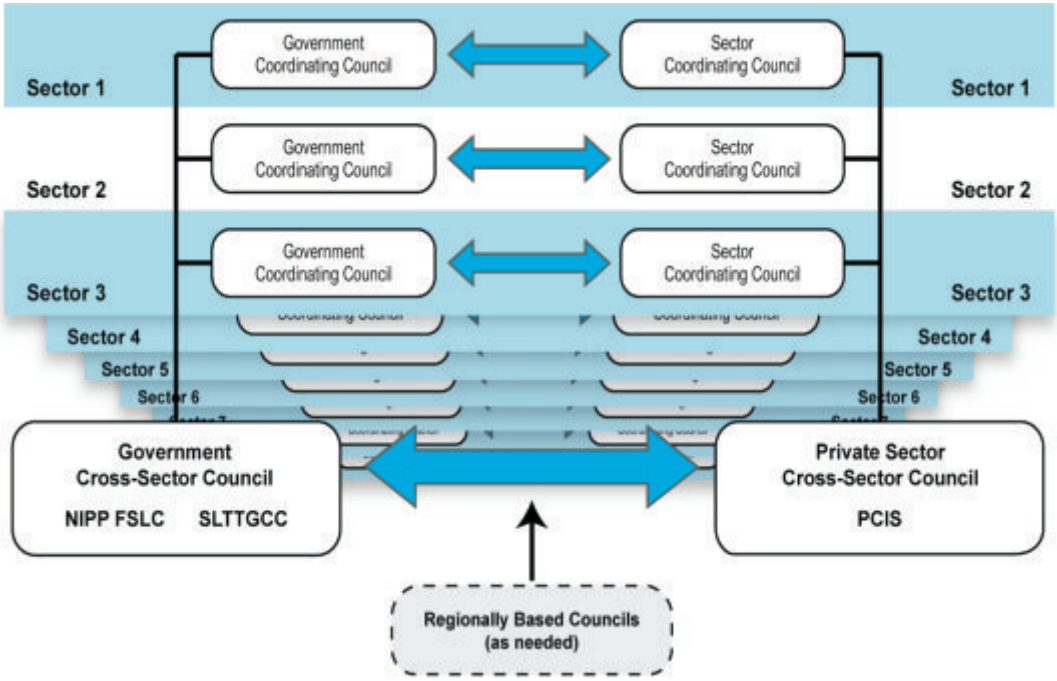
Introduction

The protection of the Nation's critical infrastructure and key resources (CIKR) requires an effective partnership framework that fosters integrated, collaborative engagement and interaction among public and private sector security partners. The Department of Homeland Security (DHS) Office of Infrastructure Protection (IP), in close coordination with public and private sector security partners, leads the coordinated national effort to mitigate risk to the Nation's CIKR through the development and implementation of an effective CIKR protection program.

The Critical Infrastructure Partnership Advisory Council (CIPAC) facilitates successful coordination and collaboration among Federal, State, local, and tribal governments and diverse private sector owners and operators on CIKR protection programs and activities. The CIPAC is a partnership between government and private-sector CIKR owners and operators that engages in a range of CIKR protection activities such as planning, coordination, National Infrastructure Protection Plan (NIPP) implementation, and operational activities, including incident response, recovery, and reconstitution.

The CIPAC directly supports the sector partnership model set out in the NIPP by providing a legal framework for members of the Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs) to engage in joint CIKR protection-related activities. On March 24, 2006, the Department of Homeland Security (DHS) published a Federal Register Notice announcing the establishment of CIPAC as a Federal Advisory Committee Act (FACA)-exempt body, pursuant to Section 871 of the Homeland Security Act.

Sector Partnership Model



NIPP Partnership

The Sector Coordinating Councils (SCCs), Government Coordinating Councils (GCCs), and Sector-Specific Agencies (SSAs) have collaborated on the necessary steps to effectively mitigate risks to the Nation's CIKR. This collaboration, the National Infrastructure Protection Plan (NIPP) Partnership, yielded successful couplings between public and private sector security partners, created a vision to guide the sectors, established goals to increase security, and initiated protection programs that aim to meet the sectors' security goals. The CIPAC Annual presents the results of the NIPP collaborations for each of the 18 CIKR Sectors.

Through public and private sector partnerships the 18 CIKR Sectors have increased CIKR protection and resilience by participating in national-level exercises, conducting risk and vulnerability assessments, and strengthening the relationship of existing security organizations. The sectors have established 15 SCCs and 17 GCCs and are developing these councils for the newest sector, Critical Manufacturing. They have also broadened membership of SCCs and GCCs through enhanced public-private sector engagement, such as the State, Local, Tribal, and Territorial GCC that was created to improve coordination across jurisdictions. The development of CIPAC and supporting partnership tools has aided in the facilitation of these crucial partnerships.

The CIPAC serves as a forum for government and private sector security partners to engage in a broad spectrum of activities, such as:

- Planning, coordination, implementation, and operational issues.
- Implementation of security programs.
- Operational activities related to CIKR protection, including incident response, recovery, and reconstitution.
- Development and support of national plans, including the NIPP and the Sector-Specific Plans (SSPs).

DHS also works with cross-sector entities established to promote coordination, communications, and best practices sharing across CIKR sectors, jurisdictions, or specifically defined geographical areas. Those entities include the following:

- Partnership for Critical Infrastructure Security (PCIS)—Addresses cross-sector issues and interdependencies among the SCCs. PCIS membership is composed of one or more members and their alternates from each of the SCCs.
- Government Cross-Sector Council—Addresses cross-sector issues and interdependencies among the GCCs, and is composed of two subcouncils: the NIPP Federal Senior Leadership Council (FSLC) and the State, Local, Tribal, and Territorial Government Cross-Sector Council (SLTTGCC).
- Regional Consortium Coordinating Council—Addresses multi-jurisdictional, cross-sector, and public-private sector efforts focused on the preparedness, protection, response, and recovery of infrastructure and the associated economies within a defined population and/or geographic area.

Key Initiatives

The 18 CIKR sectors have been effective in continuing to develop and implement programs that improve the Nation's security and improve the resilience of CIKR. Public and private sector security partners are currently implementing a wide range of protective programs that meet the security goals of each sector. CIKR protection programs are making significant contributions to the mitigation of risk by assisting security partners with the identification and mitigation of vulnerabilities; implementing protective measures; increasing preparedness for facilities, systems, and surrounding communities; supporting public awareness efforts; facilitating the sharing of CIKR protection-related effective security measures and lessons learned; and enabling planning, readiness, and incident management capabilities.

"SCCs … facilitate inclusive organization and coordination of the sector's policy development regarding CIKR protection planning and preparedness, exercises and training, public awareness, and associated plan implementation activities and requirements"

National Infrastructure Protection Plan

DHS has worked with its sector security partners to add multi-jurisdictional and crosscutting geographic perspectives to the NIPP Partnership Framework, and leverage enhanced partnerships to promote joint national, sector-specific, or regional activities. In July 2008, DHS, in close coordination with regional partners, formed the Regional Corsortiums Coordinating Council (RCCC) to foster, promote, enhance, and implement cross-jurisdictional, multidisciplinary operational homeland security communication and coordination at the regional level. The individual regional consortiums will enhance the physical security, cyber security, emergency preparedness, and overall industrial/governmental continuity and resilience of one or more States, urban areas, or municipalities.

Across the 18 sectors, security partners worked together to mitigate vulnerabilities to high-risk CIKR. To facilitate this partnership DHS established the NIPP-in-Action Portal through the DHS Lessons Learned Information Sharing Web site, created a database of effective practices, and provided templates for sectors to use to develop the sector-based awareness effort. In coordination with the SLTTGCC DHS has developed a package of capabilities, tools, and training information to implement a CIKR protection capability in State Fusion Centers.

"Continued cooperation and collaboration between and among… security partners is critical to the successful implementation of [the NIPP]."

Secretary Chertoff in National Infrastructure Protection Plan

Path Forward

The sectors have effectively improved their resilience and protection to date, and they will continue taking steps to improve their overall security amid a constantly changing threat environment. Looking forward, the sectors will continue to develop priorities and activities to allocate resources to address the gaps and threats they currently face. The sectors have developed a path forward to better focus their CIKR protection efforts. Key elements include:

- Establish a robust critical infrastructure protection R&D program to identify and make available methods and tools for sector protection program activities.
- Enable trusted and protected information sharing between public and private security partners at all levels of government.
- Establish effective cross-sector coordination mechanisms to address critical interdependencies, including incident situational awareness and cross-sector incident management.

Increasing the Nation's CIKR protection and resilience is an ongoing effort between government and public and private sector security partners. This effort will continue to be successful through further collaboration and the promotion of an effective information-sharing environment.

Cross-Sector Partnerships

Partnership for Critical Infrastructure Security

"The PCIS maintains key relationships with security partners at multiple levels of government and the private sector. These strategic partnerships are essential for sharing vital information and building trust among organizations that help protect critical infrastructures."

PCIS Business Plan 2007-2009

Partnership

The Partnership for Critical Infrastructure Security (PCIS) enables the private sector owners and operators of the Nation's most critical infrastructures to collaborate on cross-sector and interdependency issues. It provides a forum to construct trusted relationships and collaboration across sectors to improve emergency readiness and build safe, secure, and resilient infrastructures. PCIS was designated as the Private Sector Cross-Sector Council in the National Infrastructure Protection Plan to provide leadership on cross-sector initiatives and critical infrastructure planning. PCIS members are leaders from each of the Sector Coordinating Councils (SCCs), and the partnership serves as an entry point for both government and private interests to seek guidance, support, and collaboration from the private sector on efforts to develop and implement protective measures.

Vision

Robust and resilient critical infrastructures enhance economic and infrastructure security and safety in the face of emerging threats and incidents of national significance.

Goals

The PCIS pursues four key goals to advance its mission to coordinate cross-sector initiatives that promote public and private efforts to help ensure secure, safe, and reliable critical infrastructure services.

- **Partnership Leadership** – Provide proactive leadership on critical infrastructure protection issues and policy that reflects a consolidated, all-sector perspective.
- **Cross-Sector Leadership** – Provide leadership in cross-sector and interdependency issues.
- **Sector Assistance** – Increase value to the SCCs and sector owners and operators.
- **PCIS Effectiveness** – Improve the organizational effectiveness and value of the PCIS.

Selected Accomplishments

The partnership's recent accomplishments include the following:

- Created the Cross-Sector Cyber Security Working Group to provide a collaborative public-private forum to address cyber security affecting multiple sectors.
- Initiated the Standing Group on National-Level Exercises to assist the government with emergency preparedness exercises. Helped with the design, objectives, scenario development, and execution in the national-level master control cell for TOPOFF 4.
- Coordinated the private sector response to a major cyber vulnerability affecting control systems.
- Improved emergency communication capabilities of PCIS members including updating for the Emergency Notification System and an internal study of the Government Emergency Telecommunications Service (GETS) and Wireless Priority System (WPS) usage for PCIS members.
- Identified opportunities to improve the sector partnership for the National Infrastructure Advisory Council.
- Prepared communication and outreach materials to increase awareness of PCIS and cross-sector issues.

Key Initiatives

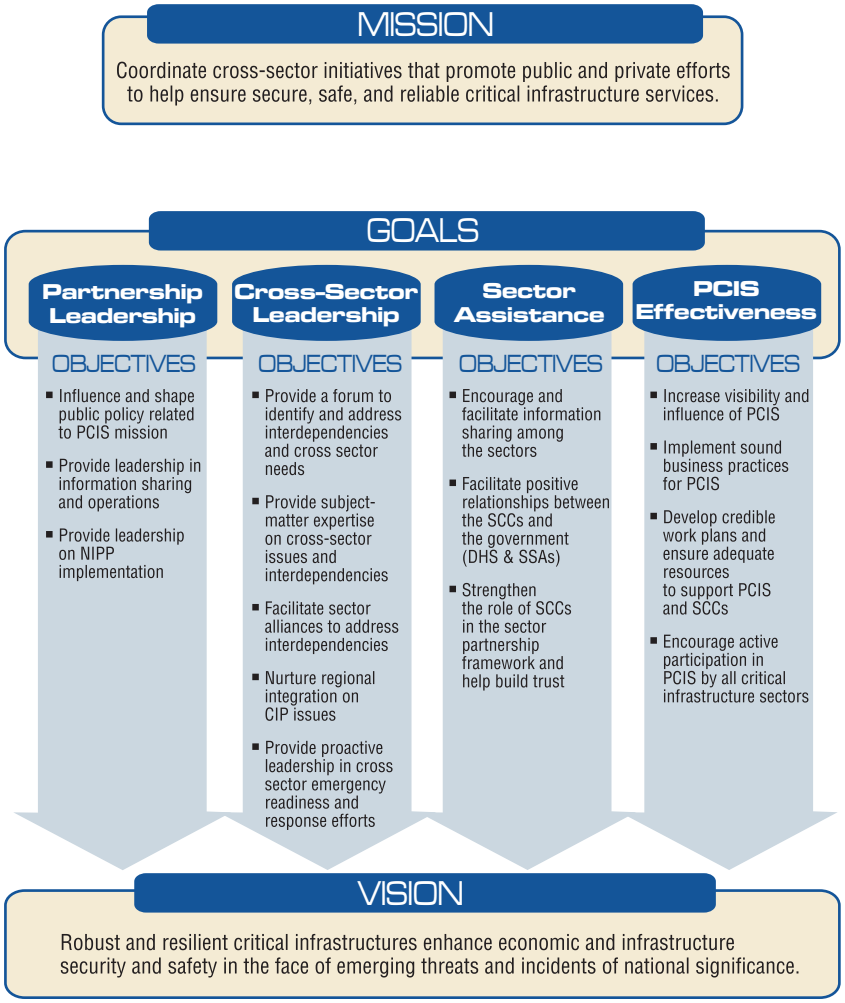
The PCIS has numerous initiatives underway, including the following:

- Conducting an internal assessment of the cross-sector readiness to the pandemic influenza threat. The assessment is intended to help each sector further refine their own pandemic planning efforts, and focus problem solving efforts on issues of common interest across the sectors, and in particular, interdependencies.
- Developing a guide to assist DHS and other government partners in engaging the CIKR sectors. The "PCIS Handbook" will provide sector descriptions and key contacts for sharing various kinds of information. The goal is to expedite information sharing between government and the right people within the sectors for strategy and policy development, operational data collection, warning and advisory posting, exercise participation, or other purposes.

Path Forward

The PCIS will continue to pursue the 15 objectives outlined in the PCIS Business Plan. Important activities for PCIS in the next year include the following:

- Coordinate State, local, and regional efforts with PCIS activities.
- Update the PCIS Business Plan and set priorities.
- Expand the reach of PCIS to additional sector partners.



Membership

- Banking and Finance
- Chemical
- Commercial Facilities
- Communications
- Dams, Locks, and Levees
- Defense Industrial Base
- Emergency Services
- Energy — Electricity
- Energy — Oil and Natural Gas
- Food and Agriculture
- Public Health and Healthcare
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Postal and Shipping
- Transportation — Aviation
- Transportation — Highway and Motor Carrier
- Transportation — Public Transit
- Transportation — Rail
- Water

The current PCIS member sectors encourage all critical sectors to join with them to achieve its mission of secure, safe, and reliable critical infrastructure services for the nation.

Federal Senior Leadership Council

Partnership

The objective of the National Infrastructure Protection Plan (NIPP) Federal Senior Leadership Council (FSLC) is to drive enhanced communications and coordination among Federal departments and agencies that have a role in implementing the NIPP and Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection. The members of the FSLC include the Sector-Specific Agencies for each of the CIKR sectors as well as several additional agencies named in HSPD-7.

Key Activities

The FSLC's primary activities include:

- Forging consensus on CIKR risk management strategies.
- Evaluating and promoting implementation of risk management-based CIKR protection programs.
- Advancing CIKR protection collaboration within and across sectors.
- Advancing CIKR protection collaboration with the international community.
- Evaluating and reporting on the progress of Federal CIKR protection activities.

Selected Accomplishments

Recent accomplishments of FSLC agencies include the following:

- Implementing their individual sector-specific plans.
- Collaborating with DHS on the Tier 1 / 2 program to ensure that high risk facilities and systems are actively managing their risks.
- Increasing engagement with state, local, tribal, territorial, and regional security partners.
- Identifying Sector-Specific Agency program management training and education needs in the areas of roles, major milestones and activities, DHS/IP organizational resources, and metrics and reporting.
- Developing the 2008 sector CIKR Protection Annual Reports (summaries follow) and measurement of performance.
- Participating in TOPOFF 4, both directly for selected sections and through a parallel exercise, Looking Glass, for members of the private sector.
- Collaborating on cyber initiatives through the cross-sector cyber security working group.

Membership

Agriculture and Food
- Department of Agriculture; Department of Health and Human Services

Banking and Finance
- Department of Treasury

Chemical
- Department of Homeland Security (DHS)/ Office of Infrastructure Protection

Commercial Facilities
- DHS/Office of Infrastructure Protection

Communications
- DHS/Office of Cyber Security and Communications

Critical Manufacturing
- DHS/Office of Infrastructure Protection

Dams
- DHS/Office of Infrastructure Protection

Defense Industrial Base
- Department of Defense

Emergency Services
- DHS/Office of Infrastructure Protection

Energy
- Department of Energy

Government Facilities
- DHS/Immigration and Customs Enforcement; Federal Protective Service

Education
- Department of Education

Information Technology
- DHS/Office of Cyber Security and Communications

National Monuments and Icons
- Department of Interior

Nuclear Reactors, Materials, and Waste
- DHS/Office of Infrastructure Protection

Postal and Shipping
- DHS/Transportation Security Administration

Public Health and Healthcare
- Department of Health and Human Services

Transportation Systems
- DHS/Transportation Security Administration; United States Coast Guard

Water
- Environmental Protection Agency

Other Federal Partners
- Departments of State, Justice, Commerce, and Transportation; Nuclear Regulatory Commission

State, Local, Tribal, and Territorial Government Coordinating Council

"The SLTGCC serves as a forum to ensure that State, local, [tribal, and Territorial] homeland security advisors or their designated representatives are fully integrated as active participants in national CIKR protection efforts."

National Infrastructure Protection Plan

"The SLTTGCC has made significant progress in establishing positive relationships with GCC sector partners, which are necessary to implement SSP initiatives."

2008 SLTTGCC Annual Report

Partnership

The State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) formed in April 2007 to better support these security partners in their implementation of the National Infrastructure Protection Plan (NIPP). The SLTTGCC strengthens the sector partnership framework by fully integrating State, local, tribal, and Territorial (SLTT) governments into the critical infrastructure and key resources (CIKR) protection process. The SLTTGCC is the second sub-council of the Government Cross-Sector Council and addresses issues and interdependencies across all sectors through the Government Coordinating Councils (GCCs). Members are geographically diverse and offer broad institutional knowledge from a wide range of professional disciplines that relate to CIKR protection. The SLTTGCC currently has five working groups to address CIKR issues of interest to State, local, tribal, and Territorial governments.

Vision

Fully integrate State, local, tribal, and Territorial governments in the critical infrastructure and key resources national strategies to assure a safe, secure, and resilient infrastructure.

Goals

SLTT security partners and DHS collaborated to develop the following six security goals, which support its overall strategic planning process:

- Promote State, local, tribal, and Territorial government's perspectives and interests in national plans and Federal planning efforts.
- Represent and promote the SLTTGCC to the State, local, tribal, and Territorial governments and federal- and private-sector security partners.
- Lead the effort to integrate CIKR SLTT government partners into the CIKR Information Sharing Environment.
- Promote the SLTT governments' perspectives and interests to DHS regarding national and regional strategies.
- Engage/leverage academic resources and the national laboratory system in furthering SLTTGCC work on behalf of SLTT governments.
- Ensure SLTT homeland security officials, or their designated representatives, are integrated fully as active participants in national CIKR protection efforts.

Selected Accomplishments and Initiatives

SLTGCC accomplishments over the past year include the following:

- Developed baseline capabilities for integrating CIKR functions into State and local fusion centers.
- Participated in the development and review of Sector Specific Plans.
- Developed a set of baseline characteristics to aid SLTT entities in identifying regional organizational partners.
- Engaged Department of Homeland Security – Infrastructure Security Compliance Division to assist in defining the Chemical-terrorism Vulnerability Information sharing process.
- Initiated membership involvement within every sector GCC to increase coordination of CIKR protection initiatives.

- Collaborated with Department of Homeland Security – Infrastructure Information Collection Division on increasing functions in Constellation/Automated Critical Asset Management System version 2.3.
- Participated in the development of the 2008 National CIKR Protection Annual Report.
- Identified need for practical how-to tools and training on how to plan and execute the activities necessary to identify, prioritize, and protect CIKR at the State, local, tribal and Territorial level.
- Identified need for educational courses to promote an understanding of the roles, responsibilities, and expectations of non-Federal governmental partners in implementing the NIPP on sector-specific and cross-sector basis.
- Developed the Homeland Security Information Network-SLTTGCC (HSIN-SLTTGCC) site and provided each working group its own portal.

Key initiatives:

- Increasing security partners' awareness of CIKR security issues and the importance of incorporating target vulnerability analysis into the current all-hazards approach of fusion centers.
- Developing the version 3.0 of Constellation/Automated Critical Asset Management System tool.
- Finalizing a seamless Chemical-terrorism Vulnerability Information sharing process with State and local security partners.
- Providing a secure, easily accessible, automated, and user-friendly tool to complete assessments and to support infrastructure data management at the State and local level.
- Increasing communication networks between SLTTGCC and its security partners to increase information sharing.

Path Forward

The SLTTGCC will take numerous steps to increase program effectiveness and advance CIKR protection guidance, strategies, and programs, including the following:

- Increase direct interface with the S&T Capstone Integrated Product Teams (IPTs) responsible for coordinating R&D activities.
- Develop metrics to measure CIKR protection performance.
- Develop a critical vulnerability information training program for State and local officials.
- Work to integrate critical infrastructure protection capabilities to the Homeland Security Exercise and Evaluation Program
- Work to integrate critical infrastructure protection capabilities into grant guidance to better reflect the all-hazards approach.
- Continue to develop and promote the Constellation/Automated Critical Asset Management System tool at all levels of government.
- Support and expand regional efforts to implement the NIPP.

Membership

- Alabama Department of Homeland Security
- Alaska Division of Homeland Security and Emergency Management
- Bloomington, MN Fire Department
- City of East Providence, RI
- Clark County, Nevada, Office of Emergency Management and Homeland Security
- Department of Public Safety, Miami Tribe of Oklahoma
- Governor s Office of Homeland Security, California
- Hennepin County, Minnesota Department of Human Services and Public Health
- Hualapai Nation Police Department
- Indianapolis/Marion County Emergency Management Agency
- Iowa Office of the Governor and Lt. Governor
- Kansas City, MO Police Department
- Michigan Department of Homeland Security
- Mohegan Tribe Department of Public Safety
- Nassau County, New York Division of Community Health for the Department of Health
- Nevada Office of Public Health Preparedness
- New Jersey Office of Homeland Security
- New Mexico Department of Homeland Security
- New York State Office of Homeland Security
- Oklahoma Office of Homeland Security
- Orlando, FL Police Department
- Port Authority of New York and New Jersey Office of Emergency Management
- St. Clair County, Michigan, Department of Emergency Management/Homeland Security
- St. Louis, Missouri, Office of Emergency Services
- Virgin Islands Office of Homeland Security

Regional Consortium Coordinating Council

"Specific regional initiatives range in scope from organizations that include multiple jurisdictions and industry partners within a single State to groups that involve jurisdictions and enterprises in more than one State and across international borders."

National Infrastructure Protection Plan

"The Pacific Northwest Economic Region provides an example of a regional organization structured as a public-private partnership that includes legislators, governments, and businesses in five States and three Canadian provinces."

National Infrastructure Protection Plan

Partnership

Regional CIKR partnerships involve multi-jurisdictional, cross-sector, and public-private sector efforts focused on the preparedness, protection, response, and recovery of infrastructure and the associated economies within a defined population and/or geographic area. Because of the specific challenges and interdependencies facing individual regions and the broad range of public- and private-sector security partners, regional efforts are often complex and diverse. To better support regional needs through implementation of the National Infrastructure Protection Plan (NIPP) at the regional level, the Department of Homeland Security (DHS) formed the Regional Consortiums Coordinating Council (RCCC) in July 2008. Members include regionally significant organizations that work toward infrastructure protection and resilience within their respective mission areas; this may include enhancing physical, cyber, and personnel security of infrastructure, emergency preparedness, and overall industrial/governmental continuity and resilience of one or more states, urban areas, or municipalities. Because coordination across government jurisdictions is crucial, the chair of State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) is a standing member of the RCCC.

Vision

Fully integrate regional consortiums into CIKR protection strategies to enhance the safety, security, and resiliency of CIKR nationwide.

Goals

The Council's security goals build on the framework articulated in the NIPP and are primarily derived from the RCCC charter. The RCCC goals include the following:

- Function as the federated framework of regionally significant organizational entities that exist to sponsor or support cooperative public-private infrastructure protection activities between and among industry; affiliated industry associations; and appropriate Federal, State, and local governments and their agencies for DHS coordination.
- Coordinate processes for implementing the two-way sharing of actionable information pertaining to physical and cyber threats, vulnerabilities, incidents, and potential protective measures among regional/local homeland security partners, DHS, the sectors within the Critical Infrastructure Partnership Advisory Council (CIPAC), and its cross-sector councils.
- Support DHS and CIKR sector partnership communication and coordination of homeland security risk mitigation and vulnerability assessment initiatives involving members of the regional consortium entities within the RCCC.
- Assist in identifying requirements for the coordination and efficient allocation of regional/local CIKR private-sector security clearances among private-sector CIKR within specific regions as required by DHS.
- Work with Federal, State, and local government agencies to properly integrate emergency preparedness activities and security responses for a terrorist attack at RCCC member facilities.
- Develop and implement an information-sharing process among RCCC members for communicating threats to or sharing situational awareness data on incidents at member facilities, including unsuccessful attacks that may provide relevant infrastructure protection data points for other regional consortium members.

- Support and encourage the coordination of specific regionally coordinated protective measures and activities to be implemented at the appropriate Homeland Security Advisory System threat level; tailor these measures to take into account geographic, regional, and specific industry factors.
- Foster ongoing coordination with DHS, State and local governments, and the CIKR sectors within CIPAC to evaluate regional interdependencies between critical infrastructure sectors that specifically impact RCCC member entities.
- Assess effective security measures of regional consortiums and their member entities and incorporate them, as appropriate, into a Council inventory accessible and available to all RCCC member entities for adoption.
- Assist in communicating Federal, State, and local initiatives, activities, and resources that may be of value to RCCC member entities in industry or government.

Selected Accomplishments

The RCCC Executive Committee drafted and approved a charter since its inception, and has prepared a draft one-year plan of activities.

Key Initiatives

The RCCC will define, develop, and implement a suite of protection-related programs and initiatives designed to prevent, deter, or mitigate threats; reduce vulnerabilities; minimize consequences; and enable timely, efficient response and recovery following an event or incident. The Council will work with all relevant infrastructure protection community partners to develop these components.

Path Forward

Existing regional consortiums, such as the Pacific Northwest Economic Region, Chicago First, Southeast Region Research Initiative, and the Community and Regional Resiliency Initiative, provide a foundation for rapid progress in forming a fully functional RCCC and for addressing regional CIKR protection needs. Steps that will be taken as the RCCC moves forward in achieving its goals include the following:

- Refine and formally ratify the RCCC charter.
- Develop and obtain approval for the associated RCCC plan of action and strategic plan.
- Define and implement the RCCC governance structure and executive council.
- Finalize RCCC membership criteria and aggressively seek full membership.

RCCC Founding Members

- Chicago First
- All Hazards Consortium
- Pacific NorthWest Economic Region
- Southeast Region Research Initiative

- Full membership is to be determined.

Sector Partnerships

Banking and Finance Sector

Partnership

The Banking and Finance Sector accounts for more than 8 percent of the U.S. annual gross domestic product and forms the backbone of the global economy. The partnership's private-sector members make up the Financial Services Sector Coordinating Council (FSSCC) and the public-sector members form the Financial and Banking Information Infrastructure Committee (FBIIC). Regional partnerships have also formed to help address local needs associated with natural and man-made disasters. Assisting these efforts is the Financial Services Information Sharing and Analysis Center (FS-ISAC) which formed to share specific threat and vulnerability assessments with the private and public sectors and to share effective incident response practices with the financial services sector. The U.S. Department of the Treasury is the Sector-Specific Agency (SSA) for the Banking and Finance Sector.

Location of Regional Partnerships

Vision

To continue to improve the resilience and availability of financial services, the Banking and Finance Sector will work through its public-private partnership to address the evolving nature of threats and the risks posed by the Sector's dependency on other critical sectors.

Goals

To improve the resilience and availability of financial services, the FSSCC, FBIIC, and Treasury Department work together to achieve the following sector-specific security goals:

- Maintain its strong position of resilience, risk management, and redundant systems in the face of a myriad of intentional, unintentional, man-made, and natural threats.
- Address and manage the risks posed by the dependency of the Sector on the Telecommunications, Information Technology (IT), Energy, and Transportation Sectors.
- Work with the law enforcement community, the private sector, and our international counterparts to increase the level of available resources dedicated to tracking and catching criminals responsible for crimes against the Sector, including cyber attacks and other electronic crimes.

"The FBIIC, the FSSCC, and regional partnerships have conducted numerous exercises, including tabletop scenarios of man-made and natural disasters, pandemic influenza, and cyber attacks, to test the preparedness and actions of the Sector during a crisis."

Banking and Finance 2007 Sector Annual Report

Selected Accomplishments

Sector partners continue to maintain and enhance the protective posture of the Banking and Finance Sector. Some of the Sector's recent accomplishments include the following:

- Participated in national exercises involving interactions between the National Infrastructure Protection Plan (NIPP) and the National Response Framework (NRF).
- Conducted sector-specific vulnerability assessments and risk assessments.
- Held a sector-wide pandemic exercise in fall 2007 to test business continuity plans.
- Created the Government Emergency Telecommunications Service Pilot Program to promote various modes of priority communications for use during a regional or national disruption.

- Held the RPCFirst annual meeting, where members conducted a resilience exercise based on an improvised explosive device scenario and reports of terrorist threats in various cities across the country.
- Developed a mission statement for the Cyber Security Committees.

Key Initiatives

Sector initiatives range from developing and testing robust emergency communication protocols to conducting and participating in exercises.

Key initiatives within the Sector include:

- Incorporate CIKR and NRF into existing exercises.
- Continue establishing new Regional Coalitions to further develop partnerships and information sharing mechanisms within local financial services communities.
- Support independent and complementary Cyber Security Committees to strengthen cyber security and resilience.

Path Forward

Numerous steps will be taken as the Banking and Finance Sector moves forward in securing it resources. Some of these steps include the following:

- Work with the U.S. Computer Emergency Readiness Team (US-CERT), the U.S. intelligence community, and law enforcement community to share information on cyber security threats.
- Attend DHS's Federal Senior Leadership Council meetings to learn more about interdependencies and share information with senior level personnel from the other sectors.
- Collaborate with the Communications, Information Technology, Energy and Transportation sectors that are needed to meet the goals of the Sector.
- The Treasury Department, through the strong public-private partnership, will continue to prepare, mitigate, and respond to man-made and natural threats that will impact Sector.

"The FS-ISAC has a reach of more than 11,000 financial institutions; it serves as the operational arm to share information about physical and cyber incidents, as well as vulnerabilities and strategies to mitigate risk on a daily basis."

Banking and Finance 2007 Sector Annual Report

"The Sector has a strong relationship with the FSSCC and is developing relationships with the Telecommunications, Transportation, IT, and Energy Sectors by inviting them to meetings to discuss CIKR issues."

Banking and Finance 2007 Sector Annual Report

FBIIC Members

- American Council of State Savings Supervisors
- Commodity Futures Trading Commission
- Conference of State Bank Supervisors
- Farm Credit Administration
- Federal Deposit Insurance Corporation
- Federal Housing Finance Board
- Federal Reserve Bank of New York
- Federal Reserve Board
- National Association of Insurance Commissioners
- National Association of State Credit Union Supervisors
- National Credit Union Administration
- North American Securities Administration Association
- Office of Federal Housing Enterprise Oversight
- Office of the Comptroller of the Currency
- Office of Thrift Supervision
- Securities and Exchange Commission
- Securities Investor Protection Corporation
- United States Department of Treasury **CHAIR**

FSSCC Members

- American Bankers Association
- American Council of Life Insurers
- American Insurance Association
- American Society for Industrial Security International
- BITS/The Financial Services Roundtable
- Bank Administration Institut
- Bank of America
- Bank of NY/Mellon
- ChicagoFIRST
- Chicago Mercantile Exchange
- Citigroup
- The Clearing House
- CLS Group
- Consumer Bankers Association
- Credit Union National Association
- The Depository Trust & Clearing Corporation
- Fannie Mae
- Financial Industry Regulatory Authority
- Financial Information Forum
- Financial Services Information Sharing and Analysis Center
- Financial Services Technology Consortium
- Freddie Mac
- Futures Industry Association
- Goldman Sachs
- ICE Futures U.S.
- Independent Community Bankers of America
- Investment Company Institute
- JP Morgan Chase
- Managed Funds Association
- Merrill Lynch
- Morgan Stanley
- Navy Federal Credit Union
- The NASDAQ Stock Market, Inc.
- National Armored Car Association
- National Association of Federal Credit Unions
- National Futures Association
- NACHA The Electronic Payments Association
- The Options Clearing Corporation
- Securities Industry Automation Corporation
- Securities Industry and Financial Markets Association
- State Farm
- State Street Global Advisors
- Travelers
- VISA USA Inc.

Chemical Sector

Partnership

The Chemical Sector — with its nearly 1 million employees and $637 billion in annual revenues — is an integral component of the U.S. economy. The Sector converts raw materials into more than 70,000 diverse products, many of which are critical to the Nation. The partnership's private-sector members make up the Chemical Sector Coordinating Council (CSCC) and the public-sector members form the Chemical Government Coordinating Council (CGCC). The Chemical Security Branch of the Sector Specific Agency Executive Management Office within the U.S. Department of Homeland Security (DHS) Office of Infrastructure Protection (IP) serves as the Sector-Specific Agency (SSA). The Infrastructure Security Compliance Division, within the DHS IP, administers the chemical facility security regulatory activities.

"Both the CGCC and CSCC added members to their respective groups. This expansion was based on the recognition of interdependencies and the need to coordinate with additional security partners."

Chemical Sector
2007 Sector Annual Report

Vision

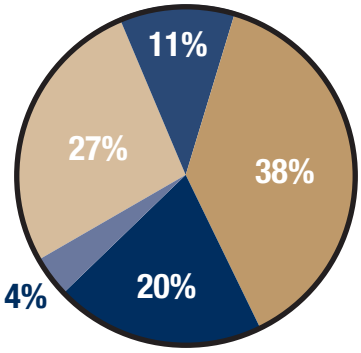
An economically competitive industry that has achieved a sustainable security posture by effectively reducing vulnerabilities and consequences of attack to acceptable levels, using risk-based assessments, industry best practices, and a comprehensive information-sharing environment between industry and government.

Goals

DHS and Chemical Sector partners have identified six overarching security goals to improve the security posture of the Sector:

- An understanding of the assets that compose the Chemical Sector; the physical, cyber, and human elements that those assets comprise; and the entities with which those assets share dependencies or interdependencies, both nationally and internationally.
- An-up-to-date risk profile of the assets that compose the Chemical Sector, set forth in a manner that supports the risk-based prioritization of critical infrastructure protection activities both within the sector and across all critical infrastructure/key resource sectors.
- An overarching, sector-wide protective program that employs measures from all facets of the protective spectrum to reduce Sector risk without hindering the economic viability of the Sector, supported by cost-effective, asset-specific protective programs targeted at the highest-risk Chemical Sector assets.
- A self-perpetuating means of measuring the progress and effectiveness of Sector critical infrastructure protection activities, including the regular preparation of reports by DHS' Sector-Specific Agency Executive Management Office for DHS senior leadership, Congress, the White House, and other relevant security partners as warranted.
- Refined processes and mechanisms for ongoing government and private sector coordination, including majority Sector participation in an information-sharing network that supports: timely dissemination of threat information to the Sector, easy reporting of suspicious activities to the government, secure communication of the assessment results to designated parties, and sharing of lessons learned and effective security practices.
- A robust critical infrastructure protection research and development (R&D) program to identify and make available methods and tools for Sector protective program activities.

Chemical Sector
Revenues By Segment



Selected Accomplishments

Sector partners continue to maintain and enhance the security posture of the Chemical Sector. Some of the Sector's accomplishments over the past year include the following:

- Completed the Pandemic Flu Contingency Planning guidance document that will assist chemical facilities in developing their own contingency plans for pandemic flu.
- Employed HSIN-Chemical to ensure that Sector partners receive alerts and bulletins from the National Infrastructure Coordination Center (NICC) and DHS.

Key Initiatives

Sector partners are already implementing numerous protective programs to meet security goals.

Key initiatives within the Sector include:

- Raising awareness through a program composed of Chemical Sector Security Summit, Chemical Boot Camp Tours, and Web-based Chemical Security Awareness Training.
- Reducing vulnerabilities by conducting Buffer Zone Protection Plans, interactive seminar and tabletop exercises, and developing cyber programs to review policies and procedures of process control systems.
- Refining methodologies (e.g., Risk Analysis and Management for Critical Asset Protection [RAMCAP]), and guidance that enable identification of Tier 1 and Tier 2 facilities.

Path Forward

Numerous steps will be taken as the Chemical Sector moves forward in securing its resources. Some of these steps include continuing to:

- Perform outreach to security partners by improving methods of communication.
- Increase awareness and training by developing training and awareness modules.
- Assess risk through the use of existing and new tools.
- Increase cyber security awareness by engaging the National Cyber Security Division.
- Participate in national exercises and maintain situational awareness for the Assistant Secretary during real incidents.
- Participate in the R&D process by maintaining awareness of R&D projects, sharing information with the Sector, and eliciting gap identification from security partners.
- Participate, oversee, and coordinate across Federal agencies the initiatives included in the Homeland Security Presidential Directive 22 (HSPD-22), *Domestic Chemical Defense*.
- Measure progress by working with the NIPP Measurement and Reporting Office (MRO) and sector partners to gather the information necessary to measure Sector progress.

"The CSCC serves as an honest broker to facilitate inclusive organization and coordination of sector policy development, infrastructure protection planning, and plan implementation activities. Such activities include sector-wide planning, sector-wide promulgation of programs and plans, development of requirements for effective information sharing, R&D, and cross-sector coordination."

Chemical Sector 2007 Sector Annual Report

"The Chemical Security Summit held in June 2007 was the sector's first DHS and CSCC co-sponsored event. The conference was attended by 350 members of the sector and has received positive feedback… the summit offered high-quality workshops and speakers who discussed the latest information regarding chemical security."

Chemical Sector 2007 Sector Annual Report

GCC Members

- Office of the Director of National Intelligence
- United States Department of Commerce
- United States Department of Defense
- United States Department of Energy
- United States Department of Homeland Security
- United States Department of Justice
- United States Department of Transportation
- United States Environmental Protection Agency

SCC Members

- The Adhesive and Sealant Council
- Agricultural Retailers Association
- American Chemistry Council
- American Forest & Paper Association
- American Petroleum Institute
- Chemical Producers & Distributors Association
- The Chlorine Institute
- Compressed Gas Association
- CropLife America
- The Fertilizer Institute
- Independent Liquid Terminals Association
- Institute of Makers of Explosives
- International Institute of Ammonia Refrigeration
- National Association of Chemical Distributors
- National Paint & Coatings Association
- National Petrochemical and Refiners Association
- Society of the Plastics Industry
- Synthetic Organic Chemical Manufacturers Association

Commercial Facilities Sector

Partnership

The Commercial Facilities Sector, widely diverse in both scope and function, is a dominant influence on the Nation's economy. The Sector consists of eight subsectors, with the Retail Subsector alone generating more than $4.4 trillion in annual sales in 2005. The Commercial Facilities Sector also includes facilities and assets (e.g., sporting stadiums, entertainment districts, and amusement and theme parks) that host activities that instill pride in the American way of life and develop a sense of community. Historically, emergency preparedness response plans for these facilities have taken place at the State and local levels, and thus asset protection cooperation with the Federal government is a relatively new concept to the Sector. The partnership's private-sector members, which include commercial facility owners, operators, and trade associations, make up the Commercial Facilities Sector Coordinating Council (CFSCC). The public-sector members form the Commercial Facilities Government Coordinating Council (CFGCC). The U.S. Department of Homeland Security serves as the Sector-Specific Agency (SSA) for the Commercial Facilities Sector.

"The Commercial Facilities SCC continues to reach out across the eight subsectors in order to increase membership within each subsector. The Commercial Facilities GCC has also examined which additional Federal, State, and local representatives could be added to its membership."

Commercial Facilities 2007 Sector Annual Report

Vision

The Commercial Facilities Sector envisions a secure, resilient, and profitable Sector in which effective and non-obstructive risk management programs instill a positive sense of safety and security in the public and sustain favorable business environments conducive to attracting and retaining employees, tenants, and customers.

Goals

To improve the security and resiliency of the Commercial Facilities Sector, the public and private sector security partners work together to achieve the following security goals:

- Enable trusted and protected information sharing between public and private security partners at all levels of government.
- Ensure that the public sector security partners disseminate timely, accurate, and threat-specific information and analysis throughout the Sector.
- Preserve the "open access" business model of most commercial facilities while enhancing overall security.
- Maintain a high level of public confidence in the security of the Sector.
- Provide security that meets the needs of the public, tenants, guests, and employees while ensuring the continued economic vitality of the owners, investors, lenders, and insurers.
- Have systems in place (e.g., emergency preparedness, training, crisis response, and business continuity plans) to ensure a timely response to and recovery from natural or man-made incidents.
- Institute a robust Sector-wide research and development (R&D) program to identify and provide independent third-party assessments of methods and tools for Sector protective program activities.
- Implement appropriate protective measures to secure cyber systems that are vital to the daily operations of the Sector.

"Many commercial facilities also house assets that belong to other critical sectors. Collaborative efforts among the 17 CIKR sectors are underway to address the issue of cascading effects stemming from sector interdependencies."

Commercial Facilities 2007 Sector Annual Report

Selected Accomplishments

Sector partners continue to maintain and enhance security and resiliency of the Sector. Some of the Sector's accomplishments over the past year include the following:

- Introduced to the Retail Subsector the Bomb-Making Awareness Program (BMAP), an awareness tool describing materials bomb makers may attempt to purchase, as well as potential "suspicious behaviors."
- Hosted the Private Sector Counterterrorism Awareness Workshop for private sector security professionals throughout the United States.
- Completed the NASCAR Mass Evacuation Planning Guide for Major Events.
- Completed the Protective Measures Guide for U.S. Sports Leagues.
- Described the requirements for CIKR-related R&D for use in the national R&D planning effort, via the 2008 Sector Annual Report.

Key Initiatives

Initiatives within the Commercial Facilities Sector range from developing plans for reinforcing public facilities' security practices to conducting workforce security training sessions.

Key initiatives within the Sector include:

- Implement a redesign of the ViSAT program.
- Developing an Evacuation Planning Guide for Stadiums in conjunction with a working group composed of SCC and GCC members, universities, and private sector partners.
- Developing Protective Measures Guides for the Retail, Lodging, and Outdoor Events Subsectors.
- Working with the Emergency Services Sector to create "Active Shooter" preparedness materials (pamphlets, posters, and pocket-size reference cards) for distribution to facilities.

Path Forward

Numerous steps will be taken as the Commercial Facilities Sector moves forward in securing its resources. Some of these steps include the following:

- Review and refine Sector security mission, vision, and goals; develop objectives.
- Review processes for prioritizing Sector infrastructure.
- Identify protective actions that can be taken to meet high-priority needs and fill gaps.
- Explore development of a Cultural Properties Subsector.
- Continue to develop a process for obtaining asset information from each subsector.
- Develop sector-specific metrics based on the goals highlighted in the Sector Business Plan.

"Vulnerability Identification Self-Assessment Tool (ViSAT) is a web-based self-assessment tool developed by DHS. Some 850 commercial facilities have access to ViSAT, and DHS has provided a grant to the International Association of Assembly Managers to promote the program."

Commercial Facilities 2007 Sector Annual Report

Commercial Facilities Subsectors

- Entertainment and Media
- Lodging
- Outdoor Events
- Public Assembly
- Real Estate
- Resorts
- Retail
- Sports Leagues

GCC Members

- National Endowment of the Arts
- United States Department of Commerce
- United States Department of Education
- United States Department of Homeland Security
- United States Department of Housing and Urban Development
- United States Department of Interior
- United States Department of Justice
- United States Environmental Protection Agency
- United States General Services Administration

SCC Members

- Affinia Hospitality
- BOMA, International
- Dallas Convention Center
- International Association of Amusement Parks & Attractions
- International Association of Assembly Managers
- International Association of Fairs and Exhibitions
- International Council of Shopping Centers
- Major League Baseball
- Marriott International
- NASCAR, Inc.
- National Association of Industrial and Office Properties
- National Association of RV Parks and Campgrounds
- National Hockey League
- National Multi Housing Council
- National Retail Federation
- NBC Universal
- Oneida Gaming Commission
- RBC Center
- Retail Industry Leaders Association
- Related Management Company
- Self Storage Association
- Stadium Management Association
- The Loss Prevention Foundation
- The Real Estate Roundtable
- Tishman Speyer Properties
- The Walt Disney Company
- Warner Bros. Studio Facilities
- Westfield Shopping Centers

Communications Sector

Partnership

The Communications Sector includes the broadcasting, cable, wireless, and wireline industries, as well as networks that support the Internet and other key information systems. There are over 35 companies and trade associations within the Communications Sector Coordinating Council (CSCC), while 7 public-sector members form the Communications Government Coordinating Council (CGCC). The National Communications System (NCS) serves as the Sector-Specific Agency (SSA). The Government is responsible for the management of Sector equities such as the National Coordinating Center (NCC) and the Network Security Information Exchange (NSIE).

"In the Communications Sector, partnerships are the foundation for all protective programs."

Communications Sector 2008 Sector Annual Report

Vision

The Communications Sector acknowledges the Nation's critical reliance on assured communications. The Communications Sector strives to ensure that the Nation's communications networks and systems are secure, resilient, and rapidly restored after a natural or manmade disaster.

Goals

Both public and private Communications Sector partners work together to achieve the following sector-specific security goals:

- Protect the overall health of the national communications backbone.
- Rapidly reconstitute critical communications services after national and regional emergencies.
- Plan for emergencies and crises by participating in exercises and updating response and continuity-of-operations plans.
- Develop protocols to manage the exponential surge in use during an emergency situation and ensure the integrity of sector networks during and after an emergency.
- Educate security partners on communications infrastructure resiliency and risk-management practices in the Communications Sector.
- Ensure timely, relevant, and accurate threat information sharing between industry and Government, including the law enforcement and intelligence communities and key decision makers in the sector.
- Establish effective cross-sector coordination mechanisms to address critical interdependencies, including incident situational awareness and cross-sector incident management.

"The Communications Sector's security practices focus on built-in resiliency, response, and recovery."

Communications Sector 2008 Sector Annual Report

Selected Accomplishments

The Communications Sector has increased its security profile with numerous accomplishments in the implementation of the Communications Sector Specific Plan (CSSP), including the following:

- Determined methods of assigning qualitative and quantitative ratings for normalizing and prioritizing architectural elements.

- Completed a National Sector Risk Assessment (NSRA).
- Increased coordination and engagement with the IT Sector, including the NSRA and Research and Development (R&D) priorities.
- Increased coordination and engagement with the Information Technology (IT) Sector, including the NSRA and Research and Development (R&D) priorities.

Key Initiatives

The Communications Sector has protective and preparedness programs, which focus strongly on response and recovery:

Key initiatives within the Sector include:

- Develop next-generation priority services to meet the evolving requirements of critical communications customers in a converged communications environment.
- Develop a Communications Sector outreach program to educate customers and other infrastructures on communications resiliency and risk-management practices.
- Focus on cyber security related programs and activities.
- Explore follow-on activities to the NSRA.

"Several physical security initiatives that are process focused, such as access to disaster sites, credentialing, security for private sector emergency responders, and emergency wireless protocols, are being addressed collaboratively by DHS/NCS and industry partners."

Communications Sector 2008 Sector Annual Report

Path Forward

The Sector will be working to determine the next steps in the implementation of the CSSP, including:

- Develop next-generation priority services to meet the evolving requirements of critical customers.
- Develop a Communications Sector outreach program.
- Focus on cyber security-related programs and activities.
- Explore follow-on activities to the NSRA.
- Develop and implement national-level protective measures to mitigate risks to nationally critical systems supporting National Security/Emergency Preparedness.
- Identify output and outcome metrics and begin collecting data.
- Solicit gap analysis of communications R&D needs and current initiatives and write a report summarizing and prioritizing the most important gaps in the Sector.

Communications Sector Relationship Map

GCC Members

- Federal Communications Commission
- National Association of Regulatory Utility Commissioners
- United States Department of Commerce
- United States Department of Defense
- United States Department of Homeland Security
- United States Department of Justice
- United States General Services Administration

SCC Members

- 3U Technologies
- Alcatel Lucent
- Americom GS
- Association of Public Television Stations
- AT&T
- BellSouth Corporation
- Boeing
- Cellular Telecommunications & Internet Association
- Cincinnati Bell
- Cingular
- Cisco
- Comcast
- Computer Sciences Corporation
- DirecTV
- Embarq
- Hughes Network Systems
- Internet Security Alliance
- Intrado
- Juniper Networks
- Level 3
- Motorola
- National Association of Broadcasters
- National Cable Television Association
- Nortel
- PAETEC
- Qwest Communications
- Rural Cellular Association
- SAVVIS
- Satellite Industry Association
- Sprint Nextel
- Telcordia
- Telecommunications Industry Association
- TeleContinuity, Inc.
- TerreStar Networks, Inc.
- Utilities Telecom Council
- US Internet Services Provider Association
- U.S. Telecom Association
- VeriSign
- Verizon

Critical Manufacturing Sector

Partnership

The Critical Manufacturing Sector is the newest sector added to the Critical Infrastructure and Key Resources (CIKR) sectors identified in the National Infrastructure Protection Plan (NIPP). The Critical Manufacturing Sector is composed of four broad manufacturing industries, which were not represented in the original 17 CIKR sectors. In 2006, these four industries employed 1.1 million workers and manufactured $676 billion in products. On March 3, 2008, the Department of Homeland Security officially designated the Critical Manufacturing Sector as an additional sector under the NIPP. The Assistant Secretary in the Office of Infrastructure Protection is currently assuming interim leadership to support the development of a Sector Coordinating Council (SCC) and Government Coordinating Council (GCC), as well as the designation of a Sector-Specific Agency (SSA) to assist in meeting the requirements of Homeland Security Presidential Directive No. 7 (HSPD-7) and the NIPP. Once this is complete, the Critical Manufacturing Sector will be able to establish partnerships and working groups among private and public security partners.

"Today's manufacturing environment is integrated into complex, interdependent supply chains. Failure in any part of a supply chain can ripple through manufacturing systems, causing cascading economic impacts."

Federal Register
Designation of the
NIPP Manufacturing Sector
April 30, 2008

Critical Manufacturing Sector Industries and Elements

Manufacturing Industry	Elements
Primary Metal Manufacturing	▪ Iron and steel mills and ferro alloy manufacturing. ▪ Alumina and aluminum production and processing. ▪ Nonferrous metal (except aluminum) production and processing.
Machinery Manufacturing	▪ Engine, turbine, and power transmission equipment.
Electrical Equipment, Appliance, and Component Manufacturing	▪ Electrical equipment.
Transportation Equipment Manufacturing	▪ Motor vehicle manufacturing. ▪ Aerospace product and parts manufacturing. ▪ Railroad rolling stock manufacturing. ▪ Other transportation equipment manufacturing.

Selected Accomplishments

The Critical Manufacturing Sector has taken initial steps in becoming a more secure and resilient sector, including the following:

- Conducted an expansive study on the manufacturing sector.
- Designated Critical Manufacturing as the 18th CIKR sector.
- Placed a notice in the Federal Register to call for public participation in the establishment and refinement of the Sector.

"Domestic manufacturers are increasingly reliant upon foreign sources of supply, energy, and on transcontinental transportation systems."

Federal Register Designation of the NIPP Manufacturing Sector April 30, 2008

Key Initiatives

The Critical Manufacturing Sector is engaged in initiatives to become more fully integrated into the CIKR Sector Partnership and to meet the NIPP goals. These initiatives will enable the Sector to further enhance its security posture.

Key initiatives within the Sector include:

- Developing the Critical Manufacturing SCC and GCC.
- Designating an SSA to assist the Sector in meeting security requirements.
- Developing and implementing the Sector-Specific Plan (SSP).
- Providing an annual report on progress in the Sector.

"Supply chains have been optimized for productivity and efficiency as opposed to redundancy, making them sensitive to disruption."

Federal Register Designation of the NIPP Manufacturing Sector April 30, 2008

Path Forward

Numerous steps will be taken as the Critical Manufacturing Sector moves forward in securing it resources, including the following:

- Engage Sector partners through meetings of the SCC and GCC.
- Develop and implement a Sector-Specific Plan.
- Identify Sector assets.
- Identify appropriate risk assessment methodologies for use by Sector partners.
- Develop Sector-specific metrics.

GCC Members

- To be determined

SCC Members

- To be determined

Dams Sector

Partnership

Dams Sector assets are vital components of the Nation's infrastructure and continuously provide a wide range of economic, environmental, and social benefits. There are approximately 82,640 dams in the United States; about 70,000 of them are regulated by State agencies, about 4,600 are regulated by Federal agencies, and the remaining dams are not regulated. More than 65 percent of dams in the United States are owned by private entities. The Dams Sector Coordinating Council (SCC) is composed of non-Federal owners and operators as well as professional organizations; the Dams Sector Government Coordinating Council (GCC) is composed of Federal owners and operators as well as Federal and State regulatory agencies and other government stakeholders. The U.S. Department of the Homeland Security (DHS), Office of Infrastructure Protection serves as the Sector-Specific Agency (SSA) for the Dams Sector.

"Dams Sector security partners leverage elements of their security practices through information sharing within and among the GCC, SCC, and Sector workgroups through periodic meetings. This information sharing is also evidenced by the development of security education outreach materials made available to all Sector security partners."

Dams Sector
2007 Sector Annual Report

Vision

The Dams Sector will identify the protective measures, strategies, and policies appropriate to protect its assets from terrorist acts through the development of multifaceted, multilevel, and flexible security programs designed to accommodate the diversity of this Sector. The Dams Sector, by fostering and guiding research in the development and implementation of protective measures, will ensure the continued economic use and enjoyment of this key resource through the use of a risk-based management program of preparedness, response, mitigation, and recovery.

Goals

To ensure the security and continued use of Sector assets, Dams Sector security partners will work together to achieve the following sector-specific security goals:

- Build Dams Sector partnership and improve communications among all Sector security partners.
- Identify Dams Sector composition, consequences, and critical assets.
- Improve Dams Sector understanding of viable threats.
- Improve Dams Sector understanding and awareness of vulnerabilities.
- Identify risks to critical assets.
- Develop guidance on how the Dams Sector will manage risks.
- Enhance the security of the Dams Sector through research and development efforts.
- Identify and address interdependencies.

"The Security Education Workgroup spearheaded development of a handbook and guide on security awareness for dam owner/operators. The Security Education Workgroup will also post templates of emergency action plans and other contingency plans on HSIN [Homeland Security Information Network] to aid owner/operators in developing such plans."

Dams Sector
2007 Sector Annual Report

Selected Accomplishments

Sector partners have taken effective measures to maintain and enhance Dams Sector security. Some of the Sector's accomplishments over the past year include the following:

- Developed a consequence-based top screen methodology to identify and characterize the subset of high-consequence facilities.

- Published a Security Awareness Handbook and a Security Awareness Guide.
- Established a Levee Sub-Sector Coordinating Council to address security and protection issues for flood damage reduction systems.

Key Initiatives

Initiatives within the Dams Sector range from studying the vulnerability of dams to aircraft impacts, to developing guidance on estimating the consequences of dam failure.

Key initiatives within the Sector include:

- Disseminating important information to owners/operators through the security and protection awareness program.
- Developing guidance for security performance, risk assessment and blast mitigation, and failure consequence estimation.
- Initiating efforts to develop security and protection strategies for levees.

Path Forward

Numerous steps will be taken as the Dams Sector moves forward in securing its resources, including the following:

- Incorporate the NIPP into strategies for cooperation with foreign countries and international/multinational organizations.
- Develop Web-based security education training tools.
- Conduct and validate consequence assessments of priority CIKR as identified by the top-screening process.
- Develop documents and reference materials to assist owners/operators in selecting protective measures and developing site security plans.
- Gather and collect information from the Dams Sector for annual reporting and national-level, cross-sector comparative analysis.
- Communicate requirements for CIKR-related research and development (R&D) to DHS for use in the national R&D planning effort.

"FERC [Federal Energy Regulatory Commission] administers the Hydro Security Program that reaches the 2,600 private and municipal hydropower dams in the Nation. All critical assets are annually inspected by FERC to ensure that security postures are appropriate to current threat levels."

Dams Sector
2007 Sector Annual Report

GCC Members

- Bonneville Power Administration
- Federal Energy Regulatory Commission
- State of California, Department of Water Resources
- State of Colorado, Division of Water Resources
- State of Nebraska, Department of Natural Resources
- State of New Jersey, Department of Environmental Protection
- State of North Carolina, Department of Environment and Natural Resources
- State of Ohio, Department of Natural Resources
- State of Pennsylvania, Department of Environmental Protection
- State of Washington, Department of Ecology
- Tennessee Valley Authority
- United States Department of Defense, Army Corps of Engineers
- United States Department of Agriculture
- United States Department of Agriculture, Bureau of Reclamation
- United States Department of Agriculture, Natural Resources Conservation Service
- United States Department of Homeland Security
- United States Department of Interior
- United States Department of Labor
- United States Department of State
- United States Department of State, International Boundary and Water Commission
- United States Department of Labor, Mine Safety and Health Administration
- Western Area Power Administration

SCC Members

- Allegheny Energy
- Ameren Services Company
- American Electric Power
- Association of State Dam Safety Officials
- Association of State Floodplain Managers
- AVISTA Utilities
- Chelan County
- CMS Energy
- Dominion Resources
- Duke Energy Corporation
- Exelon Corporation
- Hydro Québec
- National Association of Flood and Stormwater Management Agencies
- National Hydropower Association
- National Mining Association
- New York City, Department of Environmental Protection
- New York Power Authority
- Ontario Power Generation
- Pacific Gas & Electric Company
- PPL Corporation
- Progress Energy
- Scana Corporation
- Seattle City Light
- South Carolina Public Service Authority
- Southern California Edison
- Southern Company Generation
- United States Society of Dams
- Xcel Energy Corporation

Defense Industrial Base Sector

Partnership

The Defense Industrial Base (DIB) Sector includes hundreds of thousands of domestic and foreign entities and subcontractors that perform work for the Department of Defense (DOD) and other Federal departments and agencies. These firms research, develop, design, produce, deliver, and maintain military weapons systems, subsystems, components, or parts. Defense-related products and services provided by the DIB Sector equip, inform, mobilize, deploy, and sustain forces conducting military operations worldwide. As the Sector-Specific Agency (SSA), DOD leads a collaborative, coordinated effort to identify, assess, and improve risk management of critical infrastructure within the Sector. Members of these defense industry associations and DIB private sector CIKR owners and operators form the DIB Sector Coordinating Council (SCC), while the DIB Sector Government Coordinating Council (GCC) is composed of members from the U.S. Departments of Defense, Commerce, Homeland Security, Justice, and Treasury.

"DCMA [Defense Contract Management Agency] is providing outreach, education & training to DIB industry partners through its Critical Infrastructure Awareness Briefings. DCMA recently conducted its 100th Awareness Briefing with industry."

Defense Industrial Base 2008 Sector Annual Report

Vision

Ensure the ability of the DIB to support DOD missions and eliminate unacceptable risk to national security through informed infrastructure risk-management decisions.

Goals

The DIB CIPAC reviewed and approved a refined set of five Sector goals in February 2008. It also approved a set of fifteen objectives appropriately mapped to each of the goals. DIB Sector goals are:

- *Sector Risk Management:* Use an all hazards approach to manage the risk related to dependency on critical DIB assets.
- *Collaboration, Information Sharing, and Training:* Improve collaboration within a shared knowledge environment set in the context of statutory, regulatory, proprietary, and other pertinent information sharing constraints and guidance.
- *Personnel Security:* Mitigate the risk created by personnel with unescorted physical or logical access to critical DIB assets in conformance with pertinent industry best practices including regulatory and statutory requirements.
- *Physical Security:* Manage the risk created by threats to and vulnerabilities of critical DIB physical assets.

"The DCMA [Defense Contract Management Agency] is evaluating a plan to organize and train an appropriate number of reservists to undertake duties such as DIB liaison officers to the Senior Accountable Official responding to disasters and emergencies, and providing the 24/7 operations center capability to support executing DOD and national-level DIB SSA responsibilities during emergency response situations."

Defense Industrial Base 2008 Sector Annual Report

Selected Accomplishments

Sector partners continue to maintain and enhance the protective posture of the Defense Industrial Base Sector. Some of the Sector's accomplishments over the past year include the following:

- Reviewed existing risk assessment methodologies to determine compatibility with the National Infrastructure Protection Plan (NIPP) baseline criteria.

- Completed a rollout of Homeland Security Information Network–Critical Sectors communities of interest (HSIN–CS COI), which is operational, expanding registrations, and being populated with information based on SCC desires.
- Completed identification of critical DIB assets based on criteria in Homeland Security Presidential Directive-7 (HSPD-7).
- Implemented DIB Cyber Security/Information Assurance Program to increase the protection of DOD sensitive information resident on DIB networks from unauthorized disclosure.

Key Initiatives

DOD collaborates with DIB asset owners/operators to develop plans to implement protection recommendations based on the results of risk assessments. Owners/operators make risk-reduction decisions, but DOD strives to facilitate informed decision making by encouraging information sharing and making decision-support tools available.

Key initiatives within the Sector include:

- Promoting Mission Assurance Assessments to compile and implement CIKR protection approaches.
- Sharing information through the DIB Cyber Security Task Force, the Defense Security Information Exchange, and other CIPAC forums and committees.
- Implementing the "DIB Cluster" Buffer Zone Protection Program Pilot to share threat, vulnerability, and mitigation approaches.

Path Forward

Numerous steps will be taken as the Defense Industrial Base Sector moves forward in securing it resources, including the following:

- Implement policies for vetting and disseminating information to security partners.
- Complete CIPAC review and implementation of Sector metrics.
- Collaborate with other SSAs to identify cross-sector interdependencies.
- Continue DCIP Awareness Visit outreach efforts and improve coordination with DHS Physical Security Advisors.
- Continue to conduct CIP-Mission Assurance Assessments of priority DIB assets.
- Solicit feedback from critical DIB asset owners on the effectiveness and advances in infrastructure risk management practices.
- Improve classified and unclassified information-sharing capabilities throughout the Sector.

"The Department of State's Bureau of Political-Military Affairs maintains a team that coordinates with DOD to develop and implement initiatives with interagency and foreign partners to enhance the protection of the DIB, and of the international critical infrastructures on which DOD relies."

Defense Industrial Base 2007 Sector Annual Report

"The DCMA [Defense Contract Management Agency] is facilitating the Critical Infrastructure Protection Mission Assurance Assessments within the DIB sector. These full-spectrum assessments employ dedicated and specially trained teams of National Guard personnel to examine infrastructure interdependency, consequences, and vulnerabilities using a standardized protocol. In FY-07 eleven of these in-depth, on-site risk assessments were completed, and through the conclusion of FY-08 another 21 will be accomplished."

Defense Industrial Base 2008 Sector Annual Report

GCC Members

- United States Department of Commerce
- United States Department of Defense
- United States Department of Homeland Security
- United States Department of Justice
- United States Department of Treasury

SCC Members

- Aerospace Industries Association
- Alliant Techsystems
- BAE Systems
- Boeing Company
- Computer Sciences Corporation
- General Dynamics
- L3 Communications
- Lockheed Martin Corporation
- Mantech International
- National Defense Industrial Association
- Northrop Grumman Corporation
- Raytheon Company
- Science Applications International Corporation
- Washington Group International

Emergency Services Sector

Partnership

The Emergency Services Sector (ESS) is made up of a network of preparedness, response, and recovery elements that forms the Nation's first line of defense for preventing and mitigating the risk of terrorist attacks and manmade and natural disasters. The ESS encompasses a wide range of emergency response functions, whose primary missions include saving lives, protecting property and the environment, assisting communities impacted by disasters (natural or malevolent), and aiding recovery from emergency situations. The ESS has widespread involvement from a variety of entities in the public and private sectors. The primary public security partners are represented on the Emergency Services Government Coordinating Council (GCC), which is chaired by the Department of Homeland Security (DHS). The Emergency Services Sector Coordinating Council (SCC) includes the public and private sectors, and is composed of several associations that represent the major disciplines of the ESS. The SCC serves as the principal point for developing and coordinating a wide range of CIKR protection issues and activities. DHS is the Sector-Specific Agency (SSA) for the ESS.

Vision

A Sector in which facilities, key support systems, information and coordination systems, and personnel are protected from both ordinary operational risks and extraordinary risks or attacks, so that it can effectively provide a timely, coordinated, all-hazards emergency response and ensure the confidence of the citizens who depend on the Sector to protect their lives and property.

Goals

The six security goals for the ESS are to achieve/establish:

- An understanding of the physical, cyber, and human elements of the ESS assets as well as the entities with which those assets share dependencies or interdependencies, both nationally and internationally.
- An up-to-date risk profile of the assets that compose the ESS, set forth in a manner that supports the risk-based prioritization of CIKR protection activities both within the Sector and across all CIKR sectors.
- An overarching protective program that seeks to maximize the security of the Sector while minimizing the cost, burden, and any potential impact upon the Sector's ability to respond to incidents.
- A self-perpetuating means of measuring the progress and effectiveness of Sector CIKR protection activities, including regular preparation of reports by DHS for senior leadership, Congress, the White House, and other relevant security partners, as warranted.
- A robust CIKR protection R&D program to identify and make available methods and tools for Sector protective program activities.

"Mutual-aid agreements and the culture of mutual assistance and volunteerism in the emergency services help to ensure the maintenance of response capability even in the event of an incident. The availability of emergency services on a national basis is extremely difficult to disrupt due to the distributed nature of the Sector as well as established and informal assistance agreements."

Emergency Services 2008 Sector Annual Report

Emergency Services Sector Disciplines

- Law Enforcement
- Bomb Explosive Ordnance Disposal
- Special Weapons and Tactics and Tactical Operations
- Fire Service
- Emergency Medical Service
- Search and Rescue
- Urban Search and Rescue
- Emergency Management
- Hazardous Materials Response

- Refined processes and mechanisms for ongoing coordination, including majority Sector participation in an information-sharing network that supports timely dissemination of threat information to the Sector, easy reporting of suspicious activities to the government, secure communication of the assessment results to designated parties, and sharing of lessons learned and best practices.

Selected Accomplishments

Some of the Sector's accomplishments over the past year include the following:

- Developed the Tier 2 criteria, which DHS uses to identify those regions deemed most nationally significant to the Emergency Services Sector.
- Began developing the *Emergency Services Infrastructure Protection in Practice,* a document that outlines model practices that maintain and improve the Sector's ability to protect and preserve itself in an imminent or ongoing emergency.

"Protective measures in the Sector cover the full spectrum of activities designed to deter, devalue, detect, defend, mitigate, respond, and recover in an all-hazards environment."

Emergency Services 2007 Sector Annual Report

Key Initiatives

Initiatives within the ESS range from measures to prevent, deter, and mitigate threats to timely, effective response and restoration following terrorist attacks, natural disasters, or other incidents.

Key initiatives within the Sector include:

- Continuing to refine the Emergency Services Sector Risk Methodology.
- Expanding information sharing by developing programs and initiatives tailored to improve information dissemination, cyber security, and other concerns.
- Working with the DHS Science and Technology (S&T) Directorate to engage ESS practitioners and subject matter experts in S&T projects.

Path Forward

The Sector will continue to develop the priorities and activities outlined in this document. Specific programs and initiatives that the Sector has identified for the coming year include the following:

- Continue developing and release the *Emergency Services Infrastructure Protection in Practice*
- Coordinate with other programs across the public and private sector to continue developing and implementing the Emergency Services Sector Risk Methodology.
- Collaborate with the DHS National Cyber Security Division and other public and private entities to improve cyber security protective efforts and information sharing.
- Refine R&D priorities by involving the DHS S&T Integrated Product Teams as appropriate.
- Continue identifying and leveraging applicable databases and existing information resources to enhance ESS protective programs and initiatives.

GCC Members

- American Red Cross
- Federal Bureau of Investigation
- National Guard Bureau
- National Native American Law Enforcement Association
- United States Coast Guard
- United States Department of Transportation
- United States Fire Administration
- United States Forest Service
- United States Secret Service
- United States Department of Health and Human Services
- United States Department of Homeland Security
- United States Department of Interior
- United States Department of Justice
- United States Environmental Protection Agency

SCC Members

- International Association of Chiefs of Police
- International Association of Emergency Managers
- International Association of Fire Chiefs
- National Association of State EMS Officials
- National Emergency Management Association
- National Sheriffs Association

Energy Sector

Partnership

The Energy Sector consists of thousands of geographically dispersed electricity, oil, and natural gas assets that are connected by systems and networks. Collaboration is essential in order to secure such an interdependent infrastructure, which is owned, operated, hosted, and regulated by public and private entities. The Sector's public-private partnership addresses security issues and shares information on threats, vulnerabilities, and protective measures. Private-sector security partners are represented by the Electricity and Oil and Natural Gas Sector Coordinating Councils (SCCs), while public-sector security partners make up the Energy Government Coordinating Council (GCC). The Electricity SCC represents 95 percent of the electric power industry, and the Oil and Natural Gas SCC represents 98 percent of its industry. The Department of Energy serves as the Sector-Specific Agency (SSA).

"The Roadmap to Secure Control Systems in the Energy Sector establishes four main cyber security goals and addresses the full spectrum of cyber security priorities in the Energy Sector, including effective practices, standards, tools, information sharing, and training."

Energy
2007 Sector Annual Report

Vision

To establish a robust, resilient energy infrastructure in which continuity of business and services are maintained through secure and reliable information sharing, effective risk management programs, coordinated response capabilities, and trusted relationships between public and private security partners at all levels of industry and government.

Goals

To ensure a robust, resilient energy infrastructure, security partners work together to achieve the following sector-specific security goals:

- Establish robust situational awareness within the Energy Sector through timely, reliable, and secure information exchange among trusted public and private sector security partners.
- Use sound risk-management principles to implement physical and cyber measures that enhance preparedness, security, and resiliency.
- Conduct comprehensive emergency, disaster, and continuity of business planning, including training and exercises, to enhance reliability and emergency response.
- Clearly define critical infrastructure protection roles and responsibilities among all Federal, State, local, and private sector security partners.
- Understand key Sector interdependencies and collaborate with other sectors to address them, and incorporate that knowledge in planning and operations.
- Strengthen partner and public confidence in the Sector's ability to manage risk and implement effective security, reliability, and recovery efforts.

"Security of maritime facilities is critical in the Oil and Natural Gas Sector because the United States imports more than 60% of petroleum and more than 13% of refined petroleum products. Protection and capacity of ports and harbors, as well as of rail lines and inland waterways for coal transportation, are crucial to the security of energy systems."

Energy
2007 Sector Annual Report

Selected Accomplishments

Sector partners continue to maintain and enhance the protective posture of the Energy Sector. Some of the sector's accomplishments over the past year include the following:

- Continued building and strengthening the role of existing security organizations, such as the GCC, the SCC, CIPAC, and its energy security committees and working groups.

- Encouraged voluntary industry efforts to increase the availability of critical spares for the electricity, oil and natural gas, and pipelines sub-sectors.
- Established mechanisms under CIPAC with security partners to support secure communications processes and information exchange.

Key Initiatives

The Energy Sector is implementing protective programs that range from providing assistance in cyber security for the refining and petrochemical industries, to national-level domestic and international crisis and consequence management response exercises.

Key initiatives within the Sector include:

- Managing over 110 protective programs in 2008 to address risk reduction needs across the Energy Sector.
- Implementing pipeline protective programs and initiatives to secure those CIKR essential to collection, transmission, and distribution of oil and gas.
- Implementing comprehensive reviews in collaboration with DHS and the National Guard to solidify protective measures.

Path Forward

The Energy Sector will take numerous steps to move forward in securing it resources. Some of these steps include the following:

- Develop a SCC-GCC Working Group to coordinate implementation of the *Roadmap to Secure Control Systems in the Energy Sector*.
- Work with DHS to identify and, as needed, fill gaps in existing energy information and to identify publicly available databases that could provide data to support efforts to prioritize assets.
- Continue to examine human critical resources that are integral to operating the Energy Sector, including training requirements, recruitment strategies, and ageing workforce issues.
- Engage, through the CIPAC joint energy groups, in a process to discuss approaches to describing and analyzing energy systems and interdependencies with other critical sectors.
- Continue to expand upon previously held joint exercises and training with energy security partners and other interdependent sectors.
- Identify sector-specific metrics and develop approach to collecting data.
- Establish a regular schedule of joint government/industry meetings to review existing research and development (R&D) efforts and to compare results to R&D roadmaps and study recommendations.

"With voluntary partnerships as the cornerstone of its overall strategy, the Energy Sector already has more than 90 programs sponsored by dozens of public and private organizations that support the Sector's security goals."

Energy
2007 Sector Annual Report

GCC Members

- Federal Energy Regulatory Commission
- National Association of Regulatory Utility Commissioners
- National Association of State Energy Officials
- United States Department of Agriculture
- United States Department of Defense
- United States Department of Energy
- United States Department of Homeland Security
- United States Department of Interior
- United States Department of State
- United States Department of Transportation
- United States Environmental Protection Agency

Electricity SCC Members

- Arizona Public Service Company
- Exelon Corporation
- Independent Electricity System Operator, Ontario Canada
- National Resources Canada
- National Rural Electric Cooperative Association
- North American Electric Reliability Corporation
- New York State Independent System Operator
- Reliability First Corporation
- Southern Company Services, Inc.

Oil and Natural Gas SCC Members

- American Gas Association
- American Petroleum Institute
- American Public Gas Association
- Anadarko Canada Corp.
- Anadarko Petroleum Corporation
- Association of Oil Pipe Lines
- BP
- Canadian Association of Petroleum Producers
- Canadian Energy Pipeline Association
- Chevron Corporation
- ConocoPhillips
- Domestic Petroleum Council
- Dominion Resources Inc.
- Edison Chouest Offshore, LLC
- El Paso Corp.
- ExxonMobil
- Gas Processors Association
- Independent Liquid Terminals Association
- International Association of Drilling Contractors
- Interstate Natural Gas Association of America
- Independent Petroleum Association of America
- Leffler Energy
- Marathon Petroleum Company, LLC
- National Association of Convenience Stores
- National Ocean Industries Association
- National Petrochemical & Refiners Association
- National Propane Gas Association
- NiSource, Inc.
- Offshore Marine Service Association
- Offshore Operators Committee
- Petroleum Marketers Association of America
- Rowan Companies, Inc.
- Shell Oil Company
- Shipley Stores, LLC
- Society of Independent Gas Marketers Association
- U.S. Oil & Gas Association
- Valero Energy Corporation
- Western States Petroleum Association

Food and Agriculture Sector

Partnership

The Food and Agriculture Sector comprises more than 2 million farms, 900,000 companies, and 1.1 million facilities, and accounts for roughly one-fifth of the Nation's economic activity when measured from producer inputs to the end consumer. The Sector's public-private partnership raises issues and shares information on threats, vulnerabilities, and tactics for mitigating and preventing disruptions to the Sector. The Sector Coordinating Council (SCC) includes representatives from private companies and trade associations across the farm-to-table continuum. The Government Coordinating Council (GCC) includes representatives from Federal, State, tribal, and local agricultural, food, law enforcement, and related government entities. The U.S. Department of Agriculture (USDA) has Sector-Specific Agency (SSA) responsibility for production agriculture, and shares SSA responsibilities for food safety and defense with the Department of Health and Human Services (HHS) Food and Drug Administration (FDA).

Vision

Prevent the contamination of the food supply that would pose a serious threat to public health, safety, and welfare. Provide the central focus for a steadily evolving and complex industry/Sector, with particular emphasis on the protection and strengthening of the Nation's capacity to supply safe, nutritious, and affordable food. In doing so, ensure that the industry has incorporated the concepts of Homeland Security Presidential Directive No. 7 (HSPD-7) in their own critical asset protection plans, vulnerability- or risk-reduction plans, and continuity of operations plans (COOP). The Sector will provide leadership on food, agriculture, natural resources, and related issues based on sound public policy, the best available science, and efficient management.

Goals

To protect the Nation's food supply, the Sector has set the following long-term security goals:

- Improve sector analytical methods to enhance and validate the detection of a wide spectrum of threats.
- Expand the number of laboratory systems and qualified personnel.
- Improve Sector situational awareness through enhanced intelligence communication and information sharing.
- Tailor risk-based, performance-based protection measures to the Sector's physical and cyber assets, personnel, and customer products.
- Address response and recovery at the Sector level, not just as separate enterprises.
- Enhance and improve two-way communication by using the Homeland Security Information Network (HSIN).
- Work with State and local entities to ensure that they are prepared to respond to incidents (GCC-specific goal).
- Standardize CARVER*+Shock tool (GCC-specific).

SCC Sub Councils

- Agricultural Production Inputs and Services
- Animal-Producers
- Plant-Producers
- Processors-Manufacturers
- Restaurant-Food Service
- Retail
- Warehousing-Logistics

"FSIS [Food Safety and Inspection Service] has identified microbial, chemical, and radiological agents that could be used to contaminate food. As a result, the agency has expanded the capability and capacity of its laboratories to test for key threat agents. Foods are tested randomly on a daily basis for threat agents with over 450,000 samples analyzed since 2003."

Food and Agriculture 2007 Sector Annual Report

* *CARVER is an acronym for six attributes: Criticality, Accessibility, Recuperability, Vulnerability, Effect, Recognizability.*

Selected Accomplishments

Sector partners continue to maintain and enhance the protective posture of the Food and Agriculture Sector. Some of the sector's accomplishments over the past year include the following:

- Used bilateral, trilateral, quadrilateral, APEC, and G-8 activities to provide international partners the CARVER + Shock assessment tool as well as additional food and agriculture defense materials.
- Conducted the 2007 Intentional Animal Feed Contamination Tabletop Exercise on September 25 and 26, 2007, at the Pennsylvania Emergency Management Agency (PEMA) in Harrisburg, Pennsylvania, with representatives from four states.

Key Initiatives

The Sector has a number of important programs under way to protect the Sector's critical infrastructure. The focus of these programs ranges from preparedness, surveillance, and assessment, to response and recovery activities.

Key initiatives within the Sector include:

- Expanding Food Defense Awareness Training Program through the "ALERT" Campaign and "FIRST" employee initiative.
- Leveraging Strategic Partnership Program Agroterrorism (SPPA) initiative and CARVER+Shock methodology as key approaches for conducting vulnerability assessments.
- Rolling out the Food and Agriculture Sector Criticality Assessment Tool (FASCAT) project to aid States in assessing their critical sector-specific systems and sub-systems.

Path Forward

Numerous steps will be taken as the Food & Agriculture Sector moves forward in securing its resources, including the following:

- Collaborate with international partners on critical infrastructure protection activities.
- Encourage use of sector-level information-sharing mechanisms.
- Continue food defense awareness training of Federal, State, and local regulators and the private sector to increase situational awareness.
- Develop sector-specific metrics.
- Communicate requirements for CIKR-related research and development (R&D) to DHS for use in the national R&D planning effort.

"USDA, building on existing expertise and infrastructure, continues to carry out preparedness efforts designed to increase the government's ability to detect, respond to, and recover from incidents of disease, pests, or other harmful agents."

Food and Agriculture
2007 Sector Annual Report

"The food industry is focused on finding a means for reducing the risk of acts of terrorism through both the implementation of security measures and the utilization of intervention technologies that are simultaneously capable of controlling chemicals and microorganisms from both a food safety and food defense perspective."

Food and Agriculture
2007 Sector Annual Report

GCC Members

- American Association of Veterinary Laboratory Diagnosticians
- Association of Food and Drug Officials
- Association of Public Health Laboratories
- Association of State and Territorial Health Officials
- California Department of Food and Agriculture/ National Assembly
- Centers for Disease Control and Prevention
- National Assembly of State Animal Health Officials
- National Association of City and County Health Officials
- National Association of State Departments of Agriculture
- National Environmental Health Association
- National Oceanic and Atmospheric Administration
- National Plant Board
- Navajo Nation Veterinary and Livestock Program
- Office of the Secretary of Defense, Health Affairs
- United States Department of Agriculture
- United States Department of Defense
- United States Department of Health and Human Services
- United States Department of Homeland Security
- United States Department of Justice
- United States Environmental Protection Agency
- United States Fish and Wildlife Service
- United States Food and Drug Administration

Select SCC Members

- Agricultural Retailers Association
- American Farm Bureau Federation
- American Frozen Food Institute
- CF Industries, Inc.
- CropLife America
- Food Marketing Institute
- Food Processors Association
- Grocery Manufacturers Association/ Food Products Association
- International Association of Refrigerated Warehouses
- International Dairy Foods Association
- International Food Service Distributors Association
- International In flight Food Service Association
- International Warehouse Logistics Association
- Kraft Foods Global, Inc.
- McCormick & Company, Inc.
- National Association of Convenience Stores
- National Cattlemen s Beef Association
- National Corn Growers Association
- National Grain and Feed Association
- National Milk Producers Federation
- National Pork Board
- National Pork Producers Association
- National Restaurant Association
- National Retail Federation
- National Food Service Security Council
- United Fresh Fruit & Vegetable Association
- United Fresh Produce Association
- USA Rice Federation

Government Facilities Sector

Partnership

The Government Facilities Sector (GFS) includes a wide variety of facilities owned or leased by Federal, State, local, or tribal governments, located domestically and overseas. Although some types of government facilities are exclusive to the GFS, government facilities also exist in most other sectors and responsibility for these is based on predominant use. In addition to the facilities themselves, the GFS considers elements associated with and often contained, or housed, within a facility. The GFS also includes: the Education Facilities Subsector, which covers all schools, K-12, both public and private; institutions of higher education both public and private; university-based housing; proprietary schools (such as business, computer, technical, and trade schools); and state-funded pre-kindergarten programs. The Federal Protective Service (FPS) is assigned the Sector-Specific Agency (SSA) responsibility for the GFS.

"State, local, tribal, and [T]erritorial government entities play a pivotal role in activities to reduce risk within and surrounding government facilities. They are responsible for implementing the homeland security mission, protecting public safety and welfare, and ensuring the provision of essential services to communities within their jurisdictions."

Government Facilities 2007 Sector Annual Report

Vision

To establish a preparedness posture that ensures the safety and security of government facilities located domestically and overseas so that essential government functions and services are preserved without disruption.

Goals

To ensure the safety and security of government facilities, Sector security partners work together to achieve the following sector-specific security goals:

- Implement a long-term government facility risk-management program.
- Organize and partner for government facility protection.
- Integrate government facility protection as part of the homeland security mission.
- Manage and develop the capabilities of the Government Facilities Sector.
- Maximize efficient use of resources for government facility protection.

"FEMA's regional COOP [Continuity of Operations] outreach efforts provide support for 93,410 Federal department and agency offices, 818 military installations, more than 1 million State/[T]erritorial/local offices and 87,525 local governments in 50 states and 6 territories, and 563 tribal nations."

Government Facilities 2007 Sector Annual Report

Selected Accomplishments

Sector partners continue to maintain and enhance the protective posture of the GFS. Some of the Sector's accomplishments over the past year include the following:

- Developed fact sheets defining Sector categories to support identification of facilities and distributed them to Sector security partners
- Completed sector-specific CIKR inventory guidance (included in the Sector-Specific Plan).

- Identified databases, data services and sources, and modeling capabilities with CIKR application (nearly complete).

Key Initiatives

FPS and security partners are already implementing numerous protective programs that meet the GFS's security goals. These protective programs range from visual situational awareness at major public events, to Federal Emergency Management Agency (FEMA) continuity of operations (COOP). These programs have contributed to a more secure Sector.

Key initiatives within the sector include:

- Developing an FPS Risk Assessment and Management Program to provide comprehensive data collection, management, and analysis application that facilitates the risk assessment process.
- Building a compendium of all protective standards for government facilities as they relate to the physical, human, and cyber components of infrastructure protection.
- Expanding the Sector's visual situational awareness capability by working with DHS Office of Infrastructure Protection to enable a link to LiveWave cameras within the Integrated Common Analytical Viewer.

"In 2005, the FPS [Federal Protective Service] received nearly 1,500 complaints of threats against government employees. Of these reports, more than 550 formal investigations were initiated, with 150 being presented for prosecution and 100 resulting in an arrest."

Government Facilities 2007 Sector Annual Report

Path Forward

Numerous steps will be taken as the Government Facilities Sector moves forward in securing its resources, including the following:

- Develop and issue implementation guidance for conducting vulnerability a
- Establish descriptive, output, and outcome measures for Sector performan
- Monitor, review, and update prioritization based on changes to the risk lev facilities and associated elements.
- Review and revise or develop CIKR-related plans to reinforce linkages between NIPP steady-state and NRP incident management.
- Determine and prioritize Sector R&D requirements.
- Facilitate security planning and resource allocation by sharing information regarding high-risk facilities or associated elements.

GCC Members

- Air National Guard
- Architect of the Capitol
- American Society of Mechanical Engineers
- Carnegie Mellon University Computer Emergency Response Team (CERT)
- Customs and Border Protection
- Federal Aviation Administration
- Federal Emergency Management Agency
- Federal Facilities Council
- Federal Protective Service
- General Services Administration
- Interagency Security Committee
- National Aeronautics and Space Administration
- National Archives and Records Administration
- National Center for State Courts
- National Crime Prevention Council
- National Institute of Standards and Technology
- National Park Service
- Office of Personnel Management
- Social Security Administration
- State of Nevada
- State of Washington
- United States Capitol Police
- United States Department of Agriculture
- United States Department of Commerce
- United States Department of Defense
- United States Department of Education
- United States Department of Energy
- United States Department of Homeland Security
- United States Department of Interior
- United States Department of Justice
- United States Department of Labor
- United States Department of State
- United States Department of Treasury
- United States Department of Veterans Affairs
- United States Environmental Protection Agency
- United States Navy
- United States Secret Service

Healthcare and Public Health Sector

Partnership

The Healthcare and Public Health (HPH) Sector constitutes approximately 16 percent ($2 trillion) of the gross national product (GNP) and is extremely important to both the U.S. economy and the well-being of U.S. citizens. Privately owned and operated organizations make up approximately 85 percent of the Sector and are responsible for the delivery of healthcare goods and services. The public health component is carried out largely by government agencies at the Federal, State, local, tribal, and Territorial levels. The partnership's private sector members comprise the HPH Sector Coordinating Council (SCC), while the public sector component of the partnership makes up the Government Coordinating Council (GCC). The Department of Health and Human Services (HHS) serves as the Sector-Specific Agency (SSA) for the HPH Sector.

"DHS is now championing an effort to gain Secret clearances for our SCC and GCC lead partners so that data classified at the Secret level can be shared, thus allowing our security partners to participate in more detailed threat forums as well as to gain access to the data needed to further advance protection and response efforts."

Healthcare and Public Health 2007 Sector Annual Report

Vision

The HPH Sector will achieve overall resiliency against all threats – natural and manmade. It will prevent or minimize damage to, or destruction of, the Nation's healthcare and public health infrastructure. It will preserve its ability to mount timely and effective responses and its ability to recover from both routine and emergency situations. It strives to protect its essential workforce from harm resulting from all hazards including terrorist or criminal activities, natural disasters, and from serious infectious disease outbreaks.

Goals

To ensure the resiliency of the HPH Sector, security partners work together to achieve the following sector-specific long-term security goals:

- *Workforce Sustainability:* Protect the workforce from the harmful consequences of hazards that could compromise their health and safety while carrying out their HPH roles and responsibilities. Under certain circumstances, the consideration of health and safety should be extended to the families of those workforce members required during emergency response and recovery functions.
- *Physical Security:* Deter and protect against attacks intended to destroy or degrade facilities and Sector assets.
- *Physical Security:* Protect the Sector's physical assets and critical organizational systems from the consequences of all hazards.
- *Physical Security:* Deter and protect against insider threats and security weaknesses that may result in the loss or destruction of critical organizational systems.
- *Cyber Security:* Prevent and protect against unauthorized use, disclosure, modification, or exploitation of electronic information and the systems that maintain that data.
- *Cyber Security:* Protect against threats to cyber assets that may result in disruption or denial of cyber services.
- *Service Continuity:* Protect or mitigate the consequences of disruptions to the supply chain or diversion of supplies that could significantly impair continuity of Sector operations.

"The HPH Sector is working with internal business units to expand its international partnerships and refine interdependencies with countries such as Australia, Canada, and the European Union, and with entities such as the World Health Organization (WHO)."

Healthcare and Public Health 2007 Sector Annual Report

- *Service Continuity:* Maintain the availability of supporting services and resources upon which the Sector is dependent (e.g., water, power, food, transportation, fuel).
- *Service Continuity:* Continue the provision of essential services (e.g. patient care, public health) and facilitate essential response and recovery functions both during and following an event.

Selected Accomplishments

Sector partners continue to maintain and enhance the resiliency of the HPH Sector. Some of the Sector's accomplishments over the past year include the following:

- Increased integration of infrastructure protection into national planning, response, and recovery efforts through participation in cross-sector exercises.
- Initiated the development of sector-specific metrics that leverage existing measures and are aligned with sector goals and objectives.
- Identified themes, objectives, and priorities for research and development (R&D) and modeling, simulation, and analysis (MS&A) requirements.

Key Initiatives

A variety of protective programs designed to meet the HPH Sector's security goals are already being implemented by the HPH Sector and its security partners.

Key initiatives within the Sector include:

- Enhancing information sharing to increase the value and extent of sector participation.
- Collaborating with partners by sharing capability and functional data developed through network analysis to identify critical interdependencies and essential resources.
- Identifying R&D/MS&A capability gaps for workforce sustainability and medical surge capacity.

Path Forward

Numerous steps have been planned or initiated by the HPH Sector to reduce consequences or minimize the impacts resulting from all hazards. Some of these steps include:

- Assess procedures for collecting, validating, and updating CIKR protection and preparedness-related data to assure that the processes are cost-effective, meet Homeland Security Presidential Directive No. 7 (HSPD-7) needs, and are not burdensome.
- Develop a more fully integrated view of the wide range of Sector CIKR assessments.
- Develop a risk-based prioritization approach to Sector CIKR, with a focus on consequences.
- Identify a process for coordinating with other sectors to implement cross-sector programs.
- Develop a methodology to measure and assess the effectiveness of the Sector's preparedness and response capabilities to various threat scenarios and/or real events.

"The SSA actively recruits SCC and GCC members to participate in DHS- and HHS-sponsored exercises. Furthermore, SCC members who participate in State, local, and international exercises and protection and response activities share information and effective security practices with fellow SCC members."

Healthcare and Public Health 2007 Sector Annual Report

GCC Members

- Association of Public Health Laboratories
- Association of State and Territorial Health Officials
- National Association of County and City Health Officials
- National Guard Bureau
- National Indian Health Board
- State/Local Health Departments
- United States Department of Agriculture
- United States Department of Defense
- United States Department of Energy
- United States Department of Health and Human Services
- United States Department of Homeland Security
- United States Department of Veterans Affairs
- United States Environmental Protection Agency

SCC Members

- ADVAMED
- American Association of Blood Banks
- American Association of Occupational Health Nurses, Inc.
- American Hospital Association
- American Industrial Hygiene Association
- American Medical Association
- American Nurses Association
- America s Health Insurance Plans
- Association of Healthcare Resource and Materials Management Professionals
- Biotechnology Industry Organization
- Blue Cross & Blue Shield Association
- Blu Med Response Systems
- Evidence Based Research, Inc.
- Health Information and Management Systems Society
- International Cemetery and Funeral Association
- Joint Commission on Accreditation of Healthcare Organizations
- Mass Fatalities Management
- National Funeral Directors Association
- Pharmaceutical Research and Manufacturers of America

Information Technology Sector

Partnership

On a daily basis, more than $3 trillion worth of economic activity passes over secure Federal financial networks. Information Technology (IT) systems enable this economic activity, which is essential to maintaining homeland and national security. Collaboration among public and private sector security partners is critical to ensure the protection and resilience of IT Sector functions on which the Sector and Nation depend. Private-sector security partners make up the IT Sector Coordinating Council (SCC) and public-sector partners form the Government Coordinating Council (GCC). The Department of Homeland Security serves as the IT Sector-Specific Agency (SSA). The Cross-Sector Cyber Security Working Group facilitates coordination on cross-sector cyber security issues.

Vision

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 CIKR 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.

Goals

Public- and private-sector security partners collaborated to identify the following Sector goals:

- Identify, assess, and manage risks to the IT Sector's infrastructure and its international dependencies.
- 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.
- 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.

Selected Accomplishments

Sector partners continue to maintain and enhance the protective posture of the IT Sector. Some of the Sector's accomplishments over the past year include the following:

- Developed a risk assessment methodology.
- Identified critical functions and sub-functions.

Critical IT Sector Functions

- Provide IT products and services
- Provide incident management capabilities
- Provide domain name resolution services
- Provide identity management and trust support services
- Provide internet-based content, information, and communications services
- Provide internet routing, access, and connection services

"The IT Sector recognizes that collaboration among public- and private-sector security partners is critical for making progress toward achieving its goals and objectives and ensuring the protection and resilience of its critical functions on which the Sector and Nation depend."

Information Technology 2007 Sector Annual Report

- Completed a risk assessment pilot against two critical functions.
- Identified cyber security research and development (R&D) priorities.
- Contributed to the development of and participated in Cyber Storm II and TOPOFF 4.
- Developed a plan to integrate IT and Communications Sectors' operational capabilities.
- Provided leadership to the Cross-Sector Cyber Security Working Group (CSCSWG).

Key Initiatives

Initiatives within the IT Sector range from maintaining operational and situational awareness of the Nation's CIKR sectors to coordinating resources to the affected community following an incident.

Key initiatives within the Sector include:

- Developing and implementing a sector-wide risk methodology that aligns with National Infrastructure Protection Plan (NIPP) criteria.
- Managing the Protective Programs and R&D Group to facilitate awareness, promote collaboration, and identify relevant protective programs and R&D efforts.
- Addressing cross-sector cyber security by actively participating in the CSCSWG and by using protective security programs such as US-CERT, Government Emergency Telecommunications Service (GETS), and National Emergency Technology Guard (NETGuard).

Path Forward

The IT Sector has identified a clear path forward in pursuit of its CIKR protection goals, which includes the following activities:

- Conduct exercises that test the implications of a nationally significant event and the resulting public and private sector roles, responsibilities, and capabilities.
- Raise State government awareness of the IT Sector's role in CIKR protection.
- Address areas of convergence by developing an approach for a long-term regional communications and IT coordinating capability that serves all regions of the Nation.
- Develop a five-year roadmap for IT Sector R&D priorities and resource needs.
- Reassess action item prioritization based on Sector status and resource availability.
- Conduct outreach and awareness activities to increase participation in the partnership.

"The Cyber Exercise Program conducts exercises with the public and private sectors at both the national and international levels to develop, coordinate, rehearse, and refine key cyber processes; establish mechanisms for coordination and information exchange; and identify interdependencies, overlaps, and gaps to improve cyber security readiness, protection, and incident response capabilities."

Information Technology 2007 Sector Annual Report

GCC Members

- National Association of State Chief Information Officers
- United States Department of Commerce
- United States Department of Defense
- United States Department of Homeland Security
- United States Department of Justice
- United States Department of State
- United States Department of the Treasury

SCC Members

- Anakam, Inc.
- Arxan
- Business Software Alliance
- Bearing Point
- Bell Security Solutions, Inc.
- CA
- Center for Internet Security
- Cisco Systems, Inc.
- Computer and Communications Industry Association
- Computer Sciences Corporation
- Cyber Security Industry Alliance
- Computing Technology Industry Association
- Core Security
- EDS
- EMC Corporation
- EWA Information & Infrastructure Technologies, Inc.
- Electronic Industries Alliance
- Entrust, Inc.
- General Atomics
- General Dynamics
- Hatha Systems
- IBM Corporation
- Information Systems Security Association
- Information Technology Association of America
- Intel Corporation
- Information Technology Information Sharing & Analysis Center
- Information Systems Security Engineering Association
- Internet Security Alliance
- Internet Security Systems, Inc.
- International Security Trust and Privacy Alliance
- ITT Corporation
- Juniper Networks
- KPMG LLP
- Litmus Logic, LLC
- Lockheed Martin
- Lancope, Inc.
- McAfee, Inc.
- Microsoft Corporation
- NeuStar
- Northrop Grumman
- NTT America
- One Enterprise Consulting
- R & H Security Consulting LLC
- Raytheon
- Seagate Technology
- Secure Computing
- StrongAuth, Inc.
- Sun Microsystems
- System 1, Inc.
- Symantec Corporation
- TeleContinuity, Inc.
- TestPros, Inc.
- Unisys Corporation
- VeriSign
- VOSTROM

National Monuments and Icons Sector

Partnership

The National Monuments and Icons (NMI) Sector encompasses a diverse array of assets located throughout the United States and its territories. Many of these assets are listed on either the National Register of Historic Places or the List of National Historic Landmarks. All sector assets designated as NMI national critical assets are owned by the government. However, based on the primary uses of some physical structures considered as monuments or icons (e.g., Golden Gate Bridge, Hoover Dam, and the U.S. Capitol), more appropriate sectors such as Transportation Services, Commercial Facilities, Dams, or Government Facilities have been assigned the security responsibilities for these structures. The NMI Sector partnership consists of only public sector entities, though it has partnered with the Government Facilities Sector to coordinate outreach to the various State, local, tribal, and private entities through the SCC of that Sector. The Department of the Interior (DOI) serves as the Sector-Specific Agency (SSA) for the NMI Sector. DOI is responsible for approximately 1.3 million daily visitors and more than 507 million acres of public lands that include historic or nationally significant sites, dams, and reservoirs.

"As the SSA, DOI developed an assessment methodology to rate National Critical assets and the measures that could be implemented to reduce and manage risk to an acceptable level and to allow the assets to withstand specific attack scenarios. DOI has used this methodology at the NMI National Critical assets and has shared this modeling with the GCC partners."

National Monuments and Icons 2007 Sector Annual Report

Vision

The NMI Sector is dedicated to ensuring that the symbols of the Nation remain protected and intact for future generations. While protecting our landmarks, the Sector will also make certain that staff and visitors are protected from harm. Because citizen access to these monuments and icons is a hallmark of life in a free and open society, the Sector will strive for an appropriate balance between security, ease of public access, and aesthetics. However, the Sector's ultimate goal is to provide the appropriate security posture that will discourage America's adversaries from choosing our NMI assets as opportune targets.

Goals

To ensure the protection of the NMI Sector, security partners work together to achieve the following sector-specific security goals:

- Review Sector criteria to ensure a clear definition of NMI assets.
- Delineate and define roles and responsibilities for Sector security partners.
- Encourage Sector partners to perform or update risk assessments at NMI Sector assets.
- Maintain rapid and robust communications between intelligence and law enforcement agencies and GCC partners that own/operate Sector assets.
- Maintain seamless coordination among GCC partners that own/operate Sector assets.
- Maintain cross-sector coordination with regard to NMI Sector assets whose primary protective responsibility resides in another sector.
- Integrate robust security, technology, and practices contingent on agency mission priorities and available resources while preserving the appearance and accessibility of NMI Sector assets.

"OPS [Office of Protection Services] has completed an all-hazards risk assessment across all facilities and incorporated the results into the Smithsonian Institution's capital program and operations budget request."

National Monuments and Icons 2007 Sector Annual Report

- Review and update security programs that adjust to seasonal and event-specific security challenges.
- Continue to protect against insider threats.
- Update contingency response programs.

Selected Accomplishments

Sector partners continue to preserve and enhance the protective posture of the NMI Sector. Some of the Sector's accomplishments over the past year include the following:

- Completed initial CIKR consequence assessments by GCC partners.
- Addressed cross-sector vulnerabilities in the Strategic Homeland Infrastructure Risk Analysis (SHIRA) reporting criteria.
- Completed annual NIPP and SSP reviews in coordination with GCC partners.
- Coordinated CIKR-related research and development (R&D) for use in the National R&D planning effort with GCC partners, and documentation in the Sector Annual Report.

Key Initiatives

The NMI Sector is implementing a variety of protective programs, which include enhancing security in the immediate vicinity, deterring terrorists, performing independent security compliance evaluations, and completing bi-annual (or as necessary) security assessments of NMI assets. Together, these programs have contributed to a more secure sector.

Key initiatives within the sector include:

- Advancing risk management capabilities by using DOI assessment methodology and inventory taxonomy guidance to rate CIKR and develop protective measures.
- Implementing programs in alignment with NIPP partnership framework to enhance information sharing mechanisms.

Path Forward

Numerous steps will be taken as the NMI Sector moves forward in securing it resources. Some of these steps include the following:

- Review current CIKR protection measures to ensure alignment with Homeland Security Advisory System threat conditions and specific threat vectors and scenarios.
- Conduct and validate, or facilitate, consequence assessments of priority CIKR as identified by the top screening process.
- Conduct or facilitate vulnerability assessments for priority CIKR and identify cross-sector vulnerabilities.
- Communicate requirements for CIKR-related R&D to DHS for use in the national R&D planning effort.

"The National Archives Physical Security Management Program coordinates with the Washington Metropolitan Police Department and the Federal Protective Service regarding information and intelligence sharing. Additionally, the Security Management Program works with the U.S. Secret Service concerning special security events."

National Monuments and Icons 2007 Sector Annual Report

GCC Members

- National Archives and Records Administration
- Smithsonian Institution
- United States Capitol Police
- United States Department of Defense
- United States Department of Homeland Security
  - Federal Protective Service
  - Office of Infrastructure Protection
  - United States Secret Service
- United States Department of the Interior
  - National Park Service
  - Office of Law Enforcement, Security, and Emergency Management
  - United States Park Police
- United States Department of Justice
  - Federal Bureau of Investigation

Nuclear Sector

Partnership

The Nuclear Sector includes the Nation's 65 commercial nuclear power plants, which are the source of nearly 20 percent of U.S. capacity for electricity generation. The Sector also includes nuclear fuel-cycle facilities; non-power generating nuclear reactors used for research and training; nuclear and radiological materials used in medical, industrial, and academic settings; and the transportation, storage, and disposal of nuclear materials and radioactive waste. The Nuclear Sector Coordinating Council (NSCC) and Government Coordinating Council (NGCC) administer special working groups, as well as three subcouncils addressing issues specific to research and test reactors, radioisotopes, and cyber security.

"The NIPP risk management framework allows DHS to evaluate risk and partner with industry, the NRC, and DOE to help protect the assets at highest risk."

Nuclear Sector Specific Plan

Vision

The Nuclear Sector will support national security, public health and safety, public confidence, and economic stability by enhancing, where necessary and reasonably achievable, its existing high level of readiness to promote the security of the Nuclear Sector, and to lead by example to improve the Nation's overall critical infrastructure readiness.

Goals

To ensure the safety and security of the Nuclear Sector, security partners work together to achieve the following Sector security goals:

- Establish permanent and robust collaboration and communication among all security partners having security and emergency response responsibilities for the Nuclear Sector.
- Obtain information related to dependencies and interdependencies of other CIKR to the Nuclear Sector, and share it with Sector security partners.
- Increase public awareness of Sector protective measures, consequences, and proper actions following a release of radioactive material.
- Improve security, tracking, and detection of nuclear and radioactive material in order to prevent it from being used for malevolent purposes.
- Coordinate with Federal and State agencies and local law enforcement agencies to develop protective measures and tactics to deter, detect, and prevent terrorist attacks on nuclear facilities and other Nuclear Sector assets.
- Protect against the exploitation of the Nuclear Sector's cyber assets, systems, networks, and the functions they support.
- Use a risk-informed approach that includes security considerations to make budgeting, funding, and grant decisions on all identified potential protection and emergency response enhancements.
- Enhance the ability of Federal, State, local, tribal, and Territorial governments and the private sector to effectively respond to nuclear and radiological emergencies as a result of terrorist attacks, natural disasters, or other incidents.

Selected Accomplishments

Sector partners continue to maintain and enhance the safety and security of the Nuclear Sector. The Sector's accomplishments over the past year include the following:

- Completed Comprehensive Reviews (CRs) and corresponding Integrated Protective Measure Analyses at all operating U.S. nuclear power plants.
- Spearheaded development of a mechanism to provide real-time notification to relevant CIKR owner-operators in the event of a terrorist attack against a related facility.
- Continued to track and coordinate efforts to secure radioactive sources to help ensure the most efficient and effective allocation of resources.

"The Nuclear Sector sets a high standard for CIKR preparedness with its approach to security and its extensive emergency planning and exercise program around nuclear power plants."

Nuclear Sector Specific Plan

Key Initiatives

The Nuclear Sector and its security partners are already implementing numerous protective programs and initiatives, which help sustain the high-security posture characteristic of Sector facilities while addressing emerging risks affecting the Sector.

Key initiatives within the Sector include:

- Engaging Federal, State, and local partners to build on the successful completion of the Nuclear Sector CRs by accessing potential enhancements to State and local capabilities.
- Continuing efforts, in collaboration with the private sector, to further secure, or potentially replace, particularly high-risk radioisotopes used in the Healthcare Sector.
- Strengthening Sector incident-response capabilities through integrated planning and exercises that incorporate all major stakeholders.

Path Forward

Numerous steps will be taken as the Nuclear Sector moves forward in securing its resources. Some of these steps include the following:

- Continue to pursue opportunities for public-private collaboration through implementation of the NIPP risk-management framework while continually assessing, and revisiting as necessary, Sector regulations in light of the evolving risk environment.
- Strengthen cross-sector collaboration with the Healthcare, Energy, and other CIKR sectors, and further integrate State and local partners in Sector processes, as appropriate.
- Engage stakeholders to improve understanding of the Nuclear Sector and the importance of its assets in order to help prevent and mitigate potential social, psychological, and economic consequences following an incident.

GCC Members

- Conference of Radiation Control Program Directors
- Organization of Agreement States
- United States Department of Defense
- United States Department of Energy
- United States Department of Homeland Security
- United States Department of Justice
- United States Nuclear Regulatory Commission

SCC Members

- American Association of Physicists in Medicine
- Arizona Public Service Company
- Constellation Energy Generation Group
- Covidien
- Dominion Energy
- Dominion Generation
- Edlow International Company
- Entergy Operations
- Excelon Generation Company, LLC
- First Energy Corporation
- Florida Power and Light
- General Electric Energy Nuclear Energy
- National Institute of Standards and Technology
- Nuclear Energy Institute
- Oregon State University
- QSA Global
- Southern Nuclear Company
- University of Missouri Rolla
- USEC Inc.

Postal and Shipping Sector

Partnership

The Postal and Shipping Sector receives, processes, transports, and distributes billions of letters and parcels annually, and government, businesses, and private citizens rely daily on the efficient and timely functioning of the Sector. The Postal and Shipping Sector is mainly composed of four large, integrated carriers that represent 93 percent of the Sector: the United States Postal Service (USPS), the United Parcel Service (UPS), FedEx, and DHL International. The remainder of the Sector consists of smaller firms providing regional and local courier services, other mail services, mail management for corporations, and chartered air delivery services. USPS, UPS, FedEx, and DHL make up the Sector Coordinating Council (SCC), while members from the key Federal agencies form the Government Coordinating Council (GCC). The Transportation Security Administration (TSA) serves as the Sector-Specific Agency (SSA).

"Efforts to secure the Postal and Shipping Sector will realize their maximum potential only if a continuous information loop exists that engages government and the private sector in equal partnership."

Postal and Shipping 2007 Sector Annual Report

Vision

To ensure the continuity of operations, ease of use, and public confidence in the Postal and Shipping Sector by creating a multi-layered security posture that integrates public and private security partners and protective measures to deny adversaries the ability to exploit the Sector and its customers.

Goals

To ensure the continuity of operations in the Postal and Shipping Sector, security partners work together to achieve the following sector-specific security goals:

- Create Postal and Shipping Sector incident reporting mechanisms and awareness/outreach programs with the law enforcement and intelligence communities to facilitate a better understanding of the information requirements of the Sector.
- Ensure timely, relevant, and accurate threat reporting from the law enforcement and intelligence communities to key decision makers in the Sector in order to implement appropriate threat-based security measures and risk-management programs.
- Develop cross-sector coordination mechanisms to identify key interdependencies, share operational concerns, and develop protective protocols with the Transportation, Energy, Information Technology, Communications, Commercial Facilities, and Public Health sectors.
- Implement risk-based security measures for transportation assets and processing and distribution centers that are tailored to the size of implementing organizations and scalable to accommodate both routine protective requirements and periods of heightened alert.
- Work to deny terrorists the ability to exploit or replicate the trusted access that Sector personnel maintain when collecting, transporting, and delivering parcels and letters to public and private facilities.
- Work to rapidly detect, prevent further movement of, and neutralize chemical, biological, or radiological material inserted into the postal and shipping system for delivery to intended targets.
- Create public-private forums to identify roles and responsibilities for responding to a terrorist attack or other disaster and develop continuity-of-operations plans to ensure the Sector can continue to move parcels and letters to intended recipients during and after a terrorist incident or natural disaster.

"During and since the completion of the vetting process, the Transportation Security Administration (TSA) has begun to actively re-engage industry partners to implement key programs to support its identified security priorities."

Postal and Shipping 2007 Sector Annual Report

- Identify critical commodities that must be delivered to enable an effective response to a National or regionally critical emergency and develop coordinated plans to ensure such items can be delivered quickly to affected areas.
- Facilitate a close partnership with other sectors as appropriate to enable rapid identification, decontamination, and treatment of incidents in the Postal and Shipping Sector.
- Develop local, regional, and National public communication protocols to inform the American people of incidents in the Sector and minimize disruptions to their postal and shipping transactions.

Selected Accomplishments

Both public and private partners continue to maintain and enhance the protective posture of the Postal and Shipping Sector. Some of the Sector's accomplishments over the past year include the following:

- Completed a rollout of Homeland Security Information Network–Critical Sectors Communities of Interest (HSIN–CS COI).
- Established a timeline for developing sector-specific risk methodologies.
- Established protocols and approaches to obtain the data required for annual reporting and core data updates.
- Informed stakeholders about cyber security issues facing the Sector.

Key Initiatives

The Postal and Shipping Sector is implementing protective programs ranging from the creation of a registry of employees and independent contractors that have taken security awareness training, to delivering online information on industry security practices to drivers, courier company personnel, and facility personnel.

Key initiatives within the Sector include:

- Implementing a systems-based risk management process to identify, prioritize, and address CIKR risk.
- Establishing partnerships to collaboratively identify and address gaps, develop risk-based protective programs, and increase awareness.

Path Forward

Numerous steps will be taken as the Postal and Shipping Sector moves forward in securing its resources, including the following:

- Build upon ongoing government and industry cooperation through industry security groups.
- Identify existing and possibly voluntary approaches to identify, store, and protect needed postal and shipping data.
- Conduct selected asset-/facility-level, system-level, and regional-level vulnerability assessments with voluntary cooperation from the sector security partners.
- Analyze postal and shipping interdependencies with other critical sectors.
- Conduct discussions under CIPAC with stakeholder groups to identify gaps in current communications processes to speed the exchange of information on existing protective programs.
- Identify and further refine sector-specific metrics.
- Review existing R&D efforts and compare results to R&D roadmaps and study recommendations.

"The proposed voluntary Courier-Driver Registry would facilitate the Web-based registration of courier drivers, whether employees or independent contractors, that have taken security awareness training. In addition, the registry would collect driver information and validate that the driver is not a security threat (applicant's personal information will be vetted to ensure validity)."

Postal and Shipping 2007 Sector Annual Report

GCC Members

- United States Department of Defense
- United States Department of Health and Human Services
- United States Department of Homeland Security
- United States Department of Justice

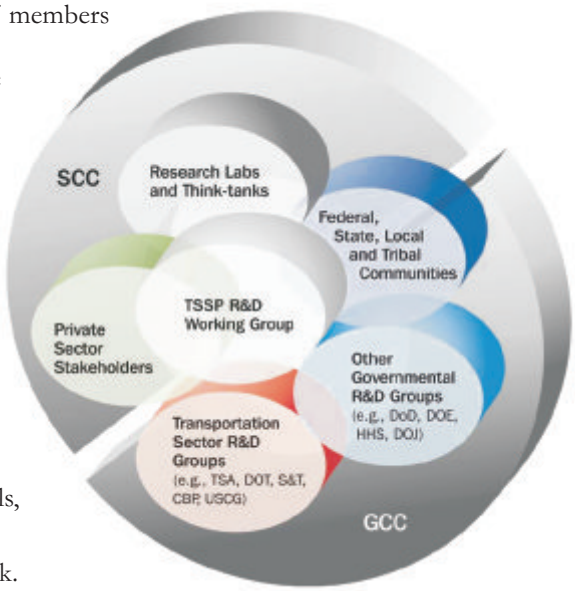
SCC Members

- DHL
- FedEx
- United Parcel Service of America, Inc.
- United States Postal Service

Transportation Systems Sector

Partnership

The Transportation Systems Sector is a vast, open network of interdependent systems that moves millions of passengers and millions of tons of goods annually. The Transportation Systems Sector partnership framework includes a Government Coordinating Council (GCC), a Sector Coordinating Council (SCC), and sub-sector GCCs and SCCs for each of the six transportation modes: Aviation, Maritime, Mass Transit, Highway, Freight Rail, and Pipeline. The SCCs include leading associations, owner-operators, and other private-sector entities with transportation security responsibilities, while the GCCs consist of members from key Federal, State and local agencies. The Transportation Security Administration (TSA) and the United States Coast Guard (USCG) serve as the Sector-Specific Agencies (SSAs) for the Transportation Systems Sector and Maritime Mode, respectively.



Transportation Systems SSP R&D Working Group

Vision

A secure and resilient transportation network, enabling legitimate travelers and goods to move without undue fear of harm or significant disruption of commerce and civil liberties.

Goals

The Transportation Sector's GCC and SCC have established the following goals, which aim to increase the Sector's security and resiliency:

- Prevent or deter acts of terrorism using or against the transportation network.
- Enhance the resilience of the transportation system.
- Improve the cost-effective use of resources for transportation security.

Selected Accomplishments

The Transportation Sector has made numerous achievements that improve the security posture of the sector. Some highlights from these accomplishments include:

- Developed and nearly completed a final review of the Transportation Security Information Sharing Plan with security partners and stakeholders.
- Expanded the Research and Development (R&D) Working Group, held regular meetings, and completed the R&D strategic plan.
- Completed 30 percent of the R&D data gathering process.
- Updated National Asset Database (NADB) transportation taxonomy and attributes to reflect a systems view of the transportation network.
- Published lists of available technologies and products related to the protection of surface transportation.
- Established the Measurement Working Group with Sector security partners.

Key Initiatives

The Transportation Sector is undertaking initiatives ranging from the creation of a highway security program to the improvement of information-sharing methods among Sector security partners.

Key initiatives within the Sector include:

- Transitioning the Port Security Exercise and Training Program (PortSTEP) into the Intermodal Security Training and Exercise Program (I-STEP), serving the surface modes and meeting 9/11 Act requirements.
- Implementing the Sector's risk management process to identify, prioritize, and address Critical Infrastructure and Key Resources (CIKR) risk with the Sector's security stakeholders.

Path Forward

Numerous steps will be taken as the Transportation Sector moves forward to secure its critical resources. Some of these steps include the following:

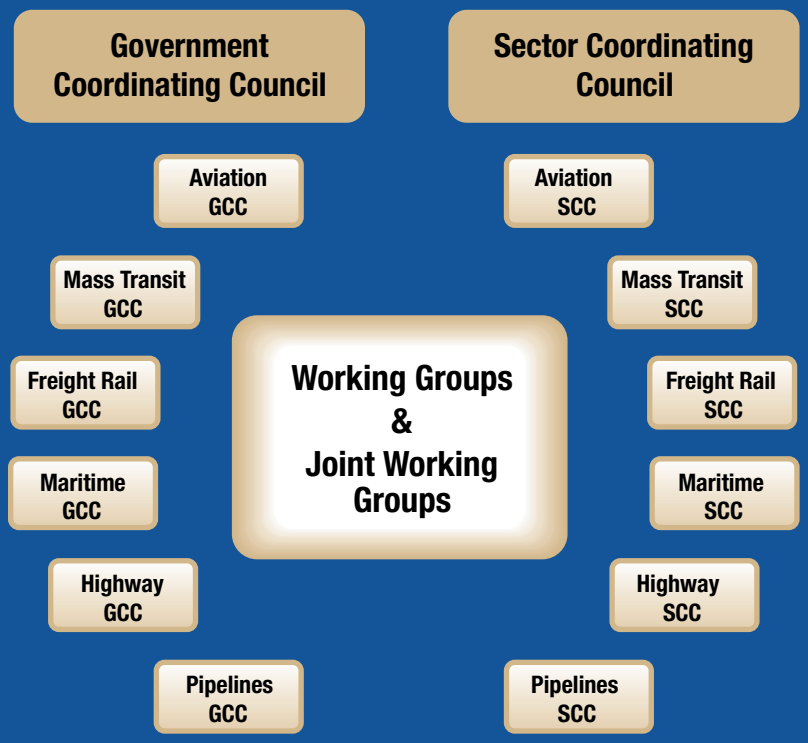
- Continue joint exercises with security partners and other interdependent sectors.
- Enhance information-sharing platforms, such as HSIN and ISACs, to share information on threats to the transportation infrastructure and security partners.
- Develop transportation system recovery and cyber security strategies through collaborative stakeholder participation in Critical Infrastructure Partnership Advisory Council working groups.

"VIPR [Visual Intermodal Protection and Response] Teams represent a cooperative effort among Federal, State, local, and industry participants to achieve a capability for flexible and unpredictable law enforcement and specialized screening missions at a variety of transportation locations. The SSA is considering methods to encourage the development and random deployments of similar teams in the State, local, and tribal jurisdictions."

Transportation 2007 Sector Annual Report

Transportation Systems Sector Partnership Framework

Due to the complexity of the sector and the number of modals involved in the partnership, this diagram is used to represent the sector's framework:



Water Sector

Partnership

There are approximately 160,000 public drinking water systems and more than 16,000 wastewater systems in the United States. Approximately 84 percent of the U.S. population receives its potable water from these drinking water systems and more than 75 percent of the U.S. population has its sanitary sewerage treated by these wastewater systems. Successful attacks on Water Sector assets could result in large numbers of illnesses or casualties, or a denial of service, which would impact public health and economic vitality. Protecting the Water Sector infrastructure requires partnerships among Federal, State, local, tribal, and Territorial governments and private-sector infrastructure owner and operators. The Water Sector Coordinating Council (SCC) was formed by eight drinking water and wastewater organizations, which appoint water utility managers to lead the SCC. The Water Sector Government Coordinating Council (GCC) enables interagency and cross-jurisdictional coordination. It is composed of representatives from Federal, State, local, tribal, and Territorial governments. The Environmental Protection Agency (EPA) serves as the Sector-Specific Agency (SSA) for the Water Sector.

Vision

The Water Sector's Security Vision is a secure and resilient drinking water and wastewater infrastructure that provides clean and safe water as an integral part of daily life. This Vision assures the economic vitality of and public confidence in the Nation's drinking water and wastewater through a layered defense of effective preparedness and security practices in the Sector.

Goals

The SCC, GCC, and EPA collaborate to achieve the followin Water Sector security goals:

- Sustain protection of public health and the environment.
- Recognize and reduce risks in the Water Sector.
- Maintain a resilient infrastructure.
- Increase communication, outreach, and public confidence.

Selected Accomplishments

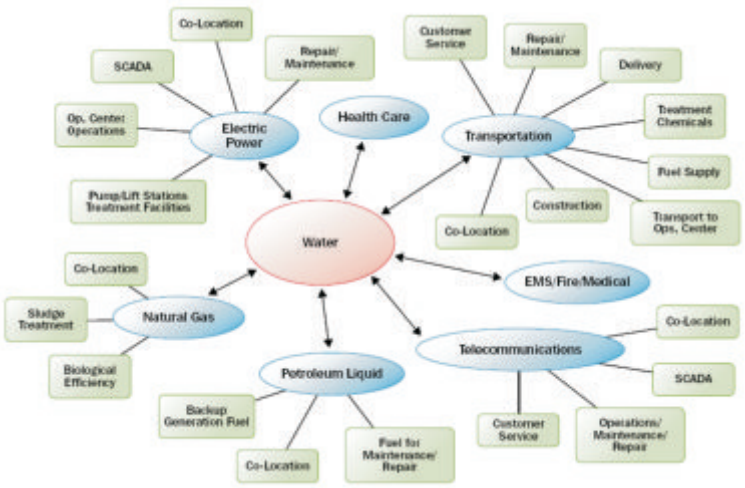
Sector partners continue to maintain and enhance the protective posture of the Water Sector. Some of the Sector's accomplishments over the past year include the follo

- Expanded the use of Water/Wastewater Agency Response (WARNs) to cover 29 states.
- Began conducting functional exercises of the Regional Laboratory Response Plans developed through the Water Laboratory Alliance.

"Partnership activities … have been achieving ongoing success…. [T]he Water Sector has increased the involvement of security partners to provide strategic direction in CIKR protection as evidenced by the expanded use of CIPAC Working Groups. Examples of these working groups include the Metrics Working Group, the Decontamination Working Group, the Cyber Security Working Group, the Research and Development (R&D) Working Group, and the Risk Assessment Working Group."

Water
2008 Sector Annual Report

Interdependencies with the Water Sector



- Developed sector-specific metrics to assess the Sector's security progress.
- Prepared a *Roadmap to Secure Control Systems in the Water Sector* that provides a strategy to mitigate the risks associated with cyber systems.

Key Initiatives

The Water Sector's protective programs and actions are interrelated and designed to strategically address the Water Sector's four security goals and associated objectives, which encompass the EPA's security program pillars of critical infrastructure protection: prevention, detection, response, and recovery. The Water Sector's protective approach enhances capabilities in all of these areas.

Key initiatives within the sector include:

- Designing and demonstrating the "Water Security Initiative"—an effective warning system for timely detection and appropriate response to drinking water contamination threats and incidents, which will have broad application to the Nation's drinking water utilities.
- Working with security partners to develop risk assessment methodologies (e.g. Risk Analysis and Management for Critical Asset Protection [RAMCAP]) that are consistent with National Infrastructure Protection Plan (NIPP) criteria.

Path Forward

Numerous steps will be taken as the Water Sector moves forward in securing its resources, including the following:

- Incorporate NIPP into strategies for cooperation with foreign countries and international/multinational organizations.
- Promote the features of an active and effective protective program within the Water Sector.
- Implement policies for vetting and disseminating information to security partners.
- Review current CIKR protection measures to ensure alignment with Homeland Security Advisory System (HSAS) threat conditions and specific threat vector and scenarios.
- Identify all databases, data services and sources, and modeling capabilities with CIKR application.
- Advise State, local, and tribal governments of SSA grant programs and/or other sources that can support NIPP.

"The path forward includes a wide array of protection efforts including collecting sector-specific metrics, making progress on cyber security and decontamination, coordinating R&D efforts, advancing business continuity planning, identifying/addressing interdependencies, and enhancing ongoing partnership efforts of the Water SCC, GCC, and CIPAC Working Groups. This path forward is aligned with the priorities and goals in the Water Sector SSP [Sector-Specific Plan]."

Water
2008 Sector Annual Report

"Water Sector's informational arm, the WaterISAC, has implemented a reporting mechanism that allows utilities to share incident information in a standardized format. Combined with other information sources, WaterISAC analysts can assess when there may be imminent threats."

Water
2007 Sector Annual Report

GCC Members

- Association of State and Interstate Water Pollution Control Administrators
- Association of State and Territorial Health Officials
- Association of State Drinking Water Administrators
- Environmental Council of the States
- National Association of County & City Health Officials
- National Association of Regulatory Utility Commissioners
- United States Army Corps of Engineers
- United States Department of Agriculture
- United States Department of Defense
- United States Department of Health and Human Services
- United States Department of Homeland Security
- United States Department of State
- United States Department of the Interior
- United States Environmental Protection Agency

SCC Members

- Association of Metropolitan Water Agencies
- American Water Works Association
- AWWA Research Foundation
- National Association of Clean Water Agencies
- National Association of Water Companies
- National Rural Water Association
- Water Environment Federation
- Water Environment Research Federation

Homeland Security