







Critical Infrastructure Partnership Advisory Council Annual

2009

Homeland Security

2009 CRITICAL INFRASTRUCTURE PARTNERSHIP ADVISORY COUNCIL ANNUAL

CONTENTS

OVERVIEW 1

CROSS-SECTOR PARTNERSHIPS 3

CIKR Cross-Sector Council 3
Federal Senior Leadership Council 5
State, Local, Tribal, and Territorial Government Coordinating Council 7
Regional Consortium Coordinating Council 9

SECTOR PARTNERSHIPS 11

Banking and Finance Sector 11
Chemical Sector 13
Commercial Facilities Sector 15
Communications Sector 17
Critical Manufacturing Sector 19
Dams Sector 21
Defense Industrial Base Sector 23
Emergency Services Sector 25
Energy Sector 27
Food and Agriculture Sector 29
Government Facilities Sector 31
Healthcare and Public Health Sector 33
Information Technology Sector 35
National Monuments and Icons Sector 37
Nuclear Sector 39
Postal and Shipping Sector 41
Transportation Systems Sector 43
Water Sector 45

OVERVIEW

INTRODUCTION

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

The sector partnership model serves as the primary organizational structure for coordinating CIKR efforts and activities. The Critical Infrastructure Partnership Advisory Council (CIPAC) directly supports the sector partnership model by providing a legal framework that enables members of the Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs) to engage in joint CIKR protection-related discussions. CIPAC serves as a forum for government and private sector partners to engage in a spectrum of activities, including:

- Planning, development, and implementation of CIKR protection and preparedness programs.
- Operational activities related to CIKR protection and resiliency, including incident response and recovery.
- Development and support of national policies and plans, including the National Infrastructure Protection Plan (NIPP) and Sector-Specific Plans (SSPs).

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

The *2009 CIPAC Annual* summarizes the infrastructure protection and resiliency activities and accomplishments of the 18 CIKR sectors and four cross-sector councils of the NIPP partnership.

NIPP PARTNERSHIP

The SCC is the principal entity for owners and operators to coordinate with the government on CIKR protection activities and issues. A GCC is formed as the government counterpart for each SCC to enable interagency and cross-jurisdictional coordination. The 18 CIKR sectors have established 16 SCCs and 18 GCCs.

Cross-sector entities promote coordination, communication, and the sharing of effective practices across CIKR sectors, jurisdictions, or specifically defined geographical areas. Those entities include the following:

- CIKR Cross-Sector Council – Addresses cross-sector issues and interdependencies among the SCCs. The Council comprises the leadership of each of the SCCs, and is housed within the privately operated Partnership for Critical Infrastructure Security (PCIS).
- Government Cross-Sector Council – Addresses inter-agency 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 Coordinating Council (SLTTGCC).
  - The FSLC consists of leadership representatives from agencies across the Federal Government that are relevant to CIKR protection and resiliency.
  - The SLTTGCC consists of homeland security directors or their equivalents from State, local, tribal and territorial governments.
- 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

Public and private sector partners are currently implementing a wide range of activities to improve the Nation's security and CIKR resiliency. These include the following:

- Enhancing information sharing through the development and operationalization of sector-wide communication and coordination procedures, supported by the Homeland Security Information Network – Critical Sectors (HSIN-CS) and other technology platforms.
- Maintaining emergency preparedness and business continuity plans.
- Participating in exercises to enhance emergency preparedness.
- Improving emergency management communication.
- Developing and distributing best practices materials.
- Raising security awareness through guidance programs, documents, or plans.
- Conducting or updating risk assessments.
- Developing and participating in CIKR protection training webinars.

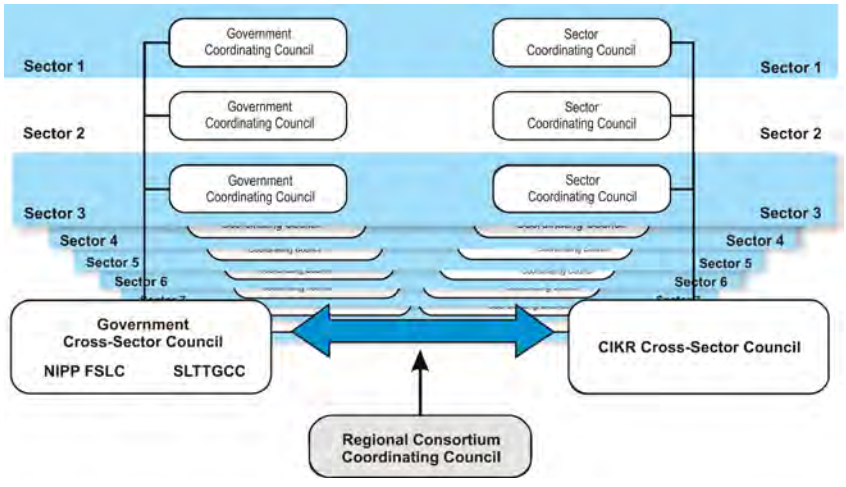
- Establishing cross-sector committees and working groups under the Cross-Sector Council within the PCIS.
- Developing an outreach program to educate State and local officials on the chemical-terrorism vulnerability information-sharing process by the SLTTGCC.
- Coordinating with the 18 CIKR sectors through the SLTTGCC to develop a program of sector liaisons that will provide regional expertise on CIKR protection and resiliency.

PATH FORWARD

Looking forward, CIKR partners will continue to grow their numbers participating in the sector partnership activities, and incorporate more and more CIKR owners and operators across the Nation into communication, information sharing and training on CIKR programs and resiliency activities. Key elements include the following:

- Expand participation in the CIKR Information Sharing Environment, and improve its effectiveness and efficiency through mission-driven requirements, including HSIN-CS.
- Improve sector awareness of interdependencies with other sectors and other agencies to help identify and address cross-sector CIKR protection gaps.
- Support private sector research and development efforts.
- Leverage existing channels of CIKR sector communication and build additional channels through state and local partnerships with CIKR owners and operators in communities.
- Disseminate products developed by the CIKR partnership to CIKR owners and operators deeper into the communities across the Nation.
- Expand the use of metrics to measure and incent progress toward sector security goals.

Sector Partnership Model



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

2009 National Infrastructure Protection Plan

"The goal of NIPP-related organizational structures, partnerships, and information-sharing networks is to establish the context, framework, and support for activities required to implement and sustain the national CIKR protection effort."

2009 National Infrastructure Protection Plan

"Prevention, response, mitigation, and recovery efforts are most efficient and effective when there is the full participation of government and industry partners; the mission suffers … without the robust participation of a wide array of CIKR partners."

2009 National Infrastructure Protection Plan

CIKR CROSS-SECTOR COUNCIL

PARTNERSHIP

The CIKR Cross-Sector Council (the Council) 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 critical infrastructure and key resources (CIKR) to improve emergency readiness and build safe, secure, and resilient infrastructures. It serves as an entry point for both government and private interests to seek input, support, and collaboration from the private sector critical infrastructure community on efforts to develop and implement critical infrastructure programs. The Council is composed of the leadership of the Sector Coordinating Councils (SCCs). The Council resides within the Partnership for Critical Infrastructure Security (PCIS), a privately operated non-profit entity.

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 Council 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 of support to the SCCs and sector owners and operators.
- Effectiveness – Improve organizational effectiveness and value.

SELECTED ACCOMPLISHMENTS

The partnership's recent accomplishments include the following:

- Conducted an internal assessment of the cross-sector readiness for the pandemic influenza threat, 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.
- Developed a guide to assist the Department of Homeland Security (DHS) and other government partners in engaging the CIKR sectors. These guidelines written and distributed within a "PCIS Handbook" provide sector descriptions and key contacts for sharing various kinds of information, expediting information sharing between government and the right people within the sectors.
- Created the Cross-Sector Cyber Security Working Group to provide a collaborative public-private forum to address cybersecurity issues 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 Top Officials 4.
- Coordinated the private sector response to a major cyber vulnerability affecting control systems.
- Identified opportunities to improve the sector partnership as input into a study being performed by the National Infrastructure Advisory Council.
- Prepared communication and outreach materials to increase awareness of the Council's activities and cross-sector issues.

KEY INITIATIVES

The Council organizes its efforts on initiatives via committees with representation from member representatives. Currently, there are several committees underway, including the following:

- Cross-Sector Cyber Security Working Group – Co-chaired by the Council and DHS, under CIPAC, it focuses on developing collaborative approaches for improving the Nation's cybersecurity.
- Education and Outreach Committee – Monitors and educates its members on U.S. Senate and House hearings, bills, and Government Accountability Office reports that may affect the CIKR community. Also educates key stakeholders on the Council's activities and the larger critical infrastructure security effort. Maintains Council awareness of government activities related to critical infrastructure matters.
- Exercise Committee – Provides private sector critical infrastructure community input to the exercise design and implementation process within DHS and the larger exercise community.

CIKR Cross Sector Council Members

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

- Interdependencies Committee – Works to identify and better understand interdependencies within the critical infrastructure community and foster better communications and collaboration between interdependent sectors.
- Regional, State, and Local Information Sharing Committee – The purpose of the Committee is to help create security and all-hazard information sharing networks at the regional, state, and local levels. This purpose includes assisting with the coordination of information sharing between regional, state and national entities.
- In addition to these committees, the Council has a member serving on the Federal government's Controlled Unclassified Information Steering Committee.

PATH FORWARD

Important activities for the Council in the next year include the following:

- Coordinate State, local, and regional efforts with Council activities.
- Update planning documents and set priorities.
- Expand the reach of the Council.

"The partnership coordinates cross-sector initiatives to support CIKR protection by identifying legislative issues that affect such initiatives and by raising awareness of issues in CIKR protection."

2009 National Infrastructure Protection Plan

The current CIKR Cross-Sector Council 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 National Infrastructure Protection Plan (NIPP) Federal Senior Leadership Council (FSLC) was formed to facilitate enhanced communication, collaboration, and coordination among Federal departments and agencies with a role in implementing the NIPP and Homeland Security Presidential Directive 7 (HSPD-7): *Critical Infrastructure Identification, Prioritization, and Protection*. The members of the FSLC include the Sector-Specific Agencies (SSAs) for each of the critical infrastructure and key resources (CIKR) sectors, as well as several additional agencies named in HSPD-7.

KEY ACTIVITIES

The FSLC's primary activities include the following:

- Forging consensus on CIKR risk management strategies.
- Evaluating and promoting implementation of risk management-based CIKR protection and resiliency programs.
- Coordinating strategic issues and issue management resolution among Federal departments and agencies, and State, regional, local, tribal, and territorial partners.
- Advancing collaboration on CIKR protection and resiliency within and across sectors and with the international community.
- Participating in efforts related to the development, implementation, review/concurrence, and triennial revision of the NIPP and the Sector-Specific Plans (SSPs).
- Evaluating and reporting on the progress of Federal CIKR protection activities.

SELECTED ACCOMPLISHMENTS

Recent accomplishments of FSLC agencies include the following:

- Continued to implement individual SSPs.
- Collaborated with the Department of Homeland Security (DHS) on the Risk Prioritization Program to ensure that high-risk facilities and systems are actively managing their risks.
- Expanded engagement with State, local, tribal, territorial, and regional CIKR partners.
- Worked with partners in government and the private sector to conduct a comprehensive triennial review and revision of the SSPs.
- Supported the development and review/concurrence of the 2009 NIPP.
- Developed the 2009 Sector CIKR Protection Annual Reports (summaries follow) and measured CIKR protection progress.
- Collaborated on cyber initiatives through the Cross-Sector Cyber Security Working Group.

MEMBERSHIP

The FSLC includes members from the following Federal departments and agencies designated in HSPD-7 as SSAs.

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

OTHER FEDERAL PARTNERS

In addition, the FSLC includes members from the U.S. Departments of Commerce, Justice, State, and Transportation; the Nuclear Regulatory Commission; the Homeland Security Council; the Office of Management and Budget; and the DHS Science and Technology Directorate.

STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENT COORDINATING COUNCIL

PARTNERSHIP

The State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) was formed in April 2007 to better support these geographically diverse 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 subcouncil 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 conducts most of its activities through five working groups: Chemical-terrorism Vulnerability Information (CVI) Working Group, Communication and Coordination Working Group, Constellation/Automated Critical Asset Management System (C/ACAMS) Working Group, Information Sharing and Collaboration Working Group, and Policy and Planning Working Group.

VISION

The SLTTGCC strives to fully integrate SLTT governments in the CIKR national strategies to assure a safe, secure, and resilient infrastructure.

GOALS

SLTT security partners and the U.S. Department of Homeland Security (DHS) collaborated to establish the following SLTTGCC security goals, which support the Council's overall strategic planning process:

- Ensure State, local, tribal, and territorial homeland security officials or their designated representatives are integrated fully as active participants in national CIKR protection efforts.
- Promote improvements in the regional coordination of SLTT governments by encouraging the integration of SLTT government perspectives into Federal planning efforts and interest in greater regional coordination with DHS and other Sector-Specific Agencies.
- Expand outreach efforts to SLTT governments, and Federal and private sector partners to increase awareness of the SLTTGCC and expand collaboration efforts.
- Lead the effort to integrate CIKR State, local, tribal, and territorial government partners into the CIKR information-sharing environment.
- Engage/leverage academic resources and the national laboratory system in furthering SLTTGCC work on behalf of SLTT governments.

SELECTED ACCOMPLISHMENTS

SLTTGCC accomplishments over the past year include the following:

- Established dialogue with the Infrastructure Security Compliance Division on chemical security, in particular the implementation of Chemical Facilities Anti-Terrorism Standards.
- Expanded and improved the Constellation/Automated Critical Asset Management System.
- Published CIKR baseline capabilities.
- Developed guidelines for identifying regional critical infrastructure protection (CIP) partners.
- Published a NIPP implementation guide for SLTT leaders.
- Contributed to the 2009 NIPP Revision.
- Contributed to the Tier 1/Tier 2 Criteria List.

KEY INITIATIVES

The SLTTGCC is engaged in various initiatives to advance CIKR protection, vulnerability reduction, and consequence mitigation.

Key initiatives within the Council include the following:

- Incorporating the improvement of the C/ACAMS program into the NIPP Risk Management Framework, partnering with the Homeland Infrastructure Threat and Risk Analysis Center to facilitate the Infrastructure Risk Analysis Partnership Program, and participating in the Sector-Specific Plan reviews.

SLTTGCC Members

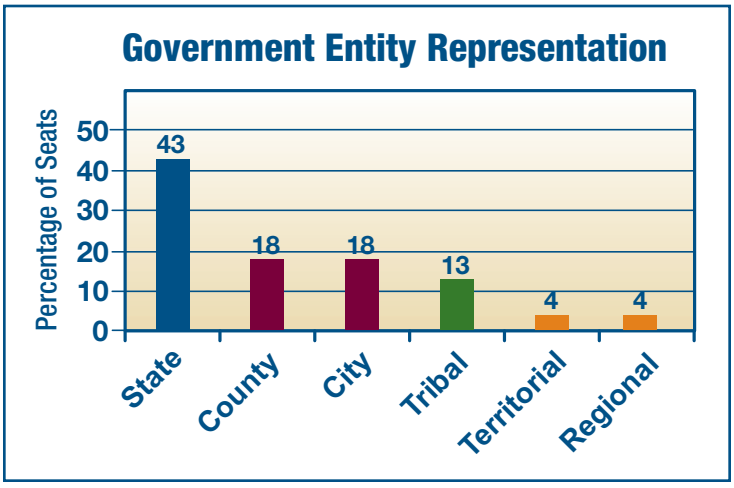
- Alabama Department of Homeland Security
- Arizona Department of Homeland Security
- Arkansas Division of Homeland Security and Emergency Management
- Bloomington, Minnesota Fire Department
- California Office of Homeland Security
- City of East Providence, Rhode Island
- City of Seattle, Washington
- Clark County, Nevada, Office of Emergency Management/Homeland Security
- Colorado State Police, Office of Preparedness and Security
- Hennepin County, Minnesota Department of Human Services and Public Health
- Hualapai Nation Police Department
- Massachusetts Office of Homeland Security
- Miami Nation

- Enhancing information sharing by refining the frequency and process by which CVI is shared, expanding the Homeland Security Information Network portal, increasing outreach efforts on the use of C/ACAMs, coordinating with regional CIKR partnerships, and increasing coordination with the sectors.
- Developing an outreach program to educate State and local officials on the chemical-terrorism vulnerability information-sharing process.
- Sending representatives to the CIP Congress to ensure that SLTT perspectives are included in any plans addressing international CIKR planning and programs.

PATH FORWARD

The SLTTGCC will continue to make progress in advancing CIKR protection guidance, strategies, and programs, including the following:

- Improve and invest in chemical security information sharing.
- Support and expand the Sector Partnership Model.
- Advocate for technical assistance to State and local CIKR partners.
- Promote the implementation of a NIPP-compliant risk management framework.
- Continue to promote the integration of CIKR protection into fusion centers.
- Ensure that SLTT perspectives are fully integrated into national strategies.



The graph above demonstrates the diversity of representation within the SLTTGCC

"The SLTTGCC currently coordinates with the RCCC [Regional Consortium Coordinating Council] to support NIPP implementation at the regional level."

2009 SLTTGCC Annual Report

"C/ACAMS is a secure, Web-based portal designed to assist State and local first responders, emergency managers, and homeland security officials in developing and implementing comprehensive CIKR protection programs."

2009 SLTTGCC Annual Report

"The SLTTGCC is collaborating with DHS, the National Fusion Center Coordinating Group, and the Criminal Intelligence Coordinating Council to integrate CIKR intelligence and analysis capabilities into fusion centers nationwide."

2009 SLTTGCC Annual Report

- Michigan Department of Information Technology
- Michigan State Police
- Montana Department of Military Affairs
- Nassau County, New York Department of Health, Office of Public Health Preparedness
- Nevada Office of Public Health Preparedness
- New Jersey Office of Homeland Security
- New York State Office of Homeland Security
- Oklahoma Office of Homeland Security
- Port Authority of New York and New Jersey Office of Emergency Management
- State of Colorado
- 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

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 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 the implementation of the National Infrastructure Protection Plan (NIPP) at the regional level, the U.S. Department of Homeland Security (DHS) formed the Regional Consortium Coordinating Council (RCCC) in July 2008. Members include regionally significant organizations that work toward infrastructure protection and resilience within their respective mission area. Because coordination across government jurisdictions is crucial, the chair of the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) is a standing member of the RCCC.

VISION

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

GOALS

The RCCC has identified the following 10 security goals:

- 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 between regional/local homeland security partners, DHS, the sectors within the Critical Infrastructure Protection Advisory Council (CIPAC), and its cross-sector councils.
- Support DHS and CIKR sector partnerships, 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 CIKR-related emergency preparedness activities and incident responses according to the National Response Framework.
- Develop and implement an information-sharing process among RCCC members for communicating threats 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 organized 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 industry-specific 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 and other preparedness measures of regional consortia 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 has accomplished the majority of its formation goals, including the following:

- Drafted and formally ratified the RCCC charter.
- Developed and obtained approval for an RCCC plan of action.
- Developed and obtained approval for an RCCC strategic plan.
- Defined, documented, and implemented the RCCC government structure.
- Defined, documented, and staffed the RCCC Executive Council.
- Selected topics for dedicated working group study.
- Finalized RCCC membership criteria.

RCCC Members

- Alaska Partnership for Infrastructure Protection
- All Hazards Consortium
- ChicagoFIRST
- Colorado Emergency Preparedness Partnership
- Colorado InfraGard
- Dallas-Fort Worth First
- InfraGard Los Angeles
- InfraGard National
- Mid-America Business Force
- Montana Critical Infrastructure Partnership

KEY INITIATIVES

The RCCC is engaged in various initiatives to advance CIKR protection, vulnerability reduction, and consequence mitigation. Key initiatives within the Council include:

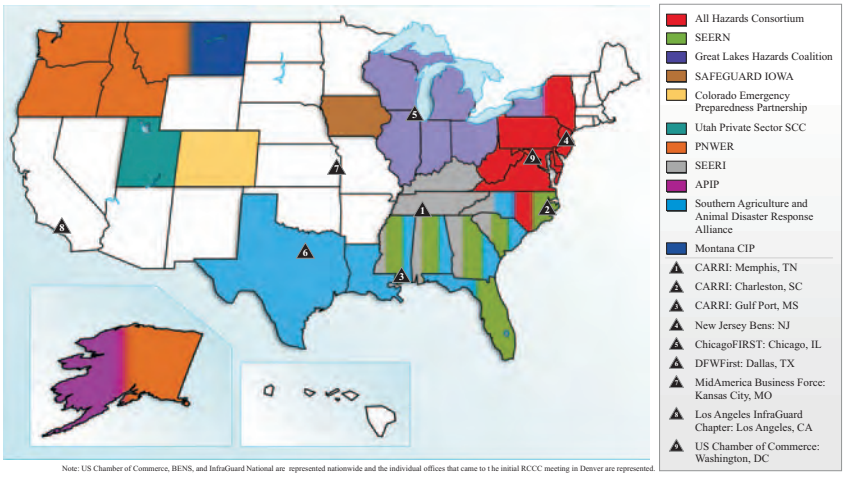
- Encouraging States and local governments to plan and execute regionally significant Homeland Security Exercise and Evaluation Program-compliant exercises.
- Reviewing Sector-Specific Plans and Sector Annual Reports to ensure that critical infrastructure protection initiatives are adequately addressed and represented.
- Coordinating with other cross-sector coordinating councils to ensure that regional voices are heard in critical infrastructure protection decision-making.
- Coordinating with the 18 CIKR sectors to develop a program of sector liaisons that will provide regional expertise regarding CIKR protection and resiliency.
- Developing a Homeland Security Information Network portal that allows for convenient dissemination of sensitive information to regional stakeholders.

PATH FORWARD

The RCCC has developed an aggressive plan to accelerate its maturation. Steps that will be taken as the RCCC moves forward in achieving its goals include the following:

- Focus on reaching out to the CIKR community as a whole.
- Identify additional regional partnership activities.
- Focus on inter-regional dependencies (nationwide).
- Continue to build the structures that will enable it to assist with national-level policy discussions that affect regional CIKR entities, as well as owners and operators.

Regional Consortium Coordinating Council Map of Participants



Note: US Chamber of Commerce, BENS, and InfraGuard National are represented nationwide and the individual offices that came to the initial RCCC meeting in Denver are represented.

"Over the past year, the RCCC has developed an initial operating structure while, at the same time, beginning the steps needed to fully implement the NIPP partnership and risk-management frameworks."

2009 Regional Consortium Coordinating Council Annual Report

"The RCCC's primary mission is to inject regional perspectives into the deliberative processes of numerous Federal agencies and government and sector working groups."

2009 Regional Consortium Coordinating Council Annual Report

"The RCCC provides a unique mechanism to integrate NIPP implementation on a regional scale, thereby accelerating the rate and increasing the depth of overall nationwide protection and resiliency."

2009 Regional Consortium Coordinating Council Annual Report

- New Jersey Business Force
- Pacific Northwest Economic Region
- Safeguard Iowa
- South East Regional Research Initiative
- Southeast Emergency Response Network
- Southern Agricultural and Animal Disaster Response Alliance
- U.S. Chamber of Commerce

BANKING AND FINANCE SECTOR

PARTNERSHIP

The Banking and Finance Sector forms the backbone of the global economy. The partnership's private-sector members make up the Financial Services Sector Coordinating Council (FSSCC) for Critical Infrastructure Protection and Homeland Security 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.

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 the Treasury Department work together to achieve the following sector-specific security goals:

- To maintain its current strong position of resilience, risk management, and redundant systems in the face of a myriad of international, unintentional, manmade, and natural threats.
- To address the risks posed by the dependence of the sector on the Communications, Information Technology, Energy, and Transportation Sectors.
- To work with the law enforcement community, financial regulatory authorities, the private sector, and our international counterparts to address risks and threats against the Financial Services Sector.

SELECTED ACCOMPLISHMENTS

Sector partners continue to maintain and enhance the protective posture of the Banking and Finance Sector. Examples of protective program performance accomplishments include the following:

- Conducted regular testing of the FBIIC emergency communication systems.
- Assessed dependencies on other sectors such as Transportation, Communications, Information Technology, and Energy.
- Sponsored, organized, and encouraged participation at outreach meetings for financial services representatives across the country regarding infrastructure protection issues, including how the FBIIC and the private sector operate as national partnerships, and how regional coalitions are an important part of the national strategy.

KEY INITIATIVES

Sector protective program initiatives aim to address the aforementioned security goals.

Key initiatives within the sector include:

- Enhancing information sharing for the financial regulatory community by meeting to discuss progress on research, exercises, protective measures, and emerging threats, and by coordinating with foreign regulatory agencies to improve emergency preparedness of critical financial institutions.
- Developing emergency-management communication protocols for information sharing during a crisis, with quarterly testing of protocols.
- Working with other Critical Infrastructure and Key Resources (CIKR) sectors and appropriate government agencies to address critical interdependencies,

FBIIC Members

- Department of the Treasury (Chair)
- American Council of State Savings Supervisors
- Board of Governors of the Federal Reserve System
- Commodity Futures Trading Commission
- Conference of State Bank Supervisors
- Farm Credit Administration
- Federal Deposit Insurance Corporation
- Federal Housing Finance Agency
- Federal Reserve Bank of New York
- National Association of Insurance Commissioners
- National Association of State Credit Union Supervisors
- National Credit Union Administration
- North American Securities Administrators Association
- Office of the Comptroller of the Currency
- Office of Thrift Supervision
- Securities and Exchange Commission
- Securities Investor Protection Corporation

FSSCC Members

- American Bankers Association
- American Council of Life Insurers
- American Insurance Association
- American Society for Industrial Security International
- BAI
- Bank of America
- Bank of NY/Mellon
- Barclays
- BITS/The Financial Services Roundtable
- CME Group
- ChicagoFIRST
- Citigroup

including telecommunications diversity and resilience and electrical power grid vulnerabilities.

- Meeting with and continuing to build relationships with representatives from the other sectors through the Partnership for Critical Infrastructure Security.
- Participating in DHS cyber-based exercises such as "Cyber Storm I," and in 2008 "Cyber Storm II," with the National Cyber Response Coordination Group.
- Working collaboratively with other CIKR sectors to accomplish DHS's Cross-Sector Cyber Security Working Group activities.

PATH FORWARD

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

- Participate in national and regional exercises to test and enhance the resilience of the Financial Services Sector, such as Banking and Finance Sector participation in Top Officials (TOPOFF) 4 and assistance in the planning process for TOPOFF 5.
- Encourage Financial Services Sector participants to develop, enhance, and test business continuity plans.
- Communicate with the United States Computer Emergency Readiness Team, the U.S. intelligence community, and law enforcement community to share information on cyber security threats that may directly or indirectly impact the sector.
- Coordinate with DHS to sponsor classified-level clearances for need-to-know personnel within the Financial Services Sector to facilitate the sharing of relevant information affecting the sector.
- Support a private sector R&D initiative to research ways to make Financial Services systems more resilient against cyber threats.

"The FBIIC has also reached out on a bilateral and multilateral basis to counterparts in other countries who are grappling with resilience issues."

2008 Update to the Banking and Finance Sector-Specific Plan

"As the SSA, the Treasury routinely coordinates communication tests for information sharing between the FBIIC and the private sector to ensure that communication protocols would work efficiently and effectively during an incident."

2008 Update to the Banking and Finance Sector-Specific Plan

- 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
- ICS Futures U.S.
- Independent Community Bankers of America
- Investment Company Institute
- JPMorgan Chase
- Managed Funds Association
- Merrill Lynch
- Morgan Stanley
- NACHA The Electronic Payments Association
- The NASDAQ Stock Market, Inc.
- National Armored Car Association
- National Association of Federal Credit Unions
- National Futures Association
- Navy Federal Credit Union
- NYSE Euronext
- The Options Clearing 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 revenue – 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. Pursuant to Homeland Security Presidential Directive 7 (HSPD-7), the U.S. Department of Homeland Security (DHS) is responsible for managing and coordinating Chemical Sector security activities. Within DHS, this overarching responsibility has been delegated to the National Protection and Programs Directorate (NPPD) Office of Infrastructure Protection (IP). Within IP, responsibilities for Chemical Sector security are held by two divisions. The Sector-Specific Agency Executive Management Office (SSA EMO) Chemical Branch has responsibility for overseeing voluntary security efforts by serving as the Sector-Specific Agency (SSA) for the Chemical Sector, and the Infrastructure Security Compliance Division was established to administer regulatory activities.

The Sector Coordinating Council (SCC) and Government Coordinating Council (GCC) are currently working to reevaluate and edit the Chemical Sector's security vision statement, mission statement, and goals to ensure continued relevance and commitment as the sector changes and the risk environment evolves. The revised vision statement, mission statement, and goals will be published in the 2010 Chemical Sector-Specific Plan.

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

The DHS and Chemical Sector partners have identified six overarching security goals in order 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 and key resources 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 the 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/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 program to identify and make available methods and tools for sector protective program activities.

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 Security Vulnerability Assessments at more than 5,700 high-risk chemical facilities using the Department's Chemical Security Assessment Tool.
- Spent an estimated 1 million man-hours on vulnerability assessments at high-risk facilities.
- Piloted and launched the Voluntary Chemical Assessment Tool at nine chemical facilities with a consensus that the tool was valuable and effective.
- Held a Sector-Specific Metrics Workshop, which resulted in a consensus set of draft Chemical Sector-specific metrics.
- Participated in National Level Exercise 2009 which resulted in a number of lessons learned for DHS and the sector.
- Developed the first edition *Roadmap to Secure Control Systems in the Chemical Sector.*

GCC Members

- Office of the Director of National Intelligence
- State, Local, Tribal, and Territorial GCC representatives
- U.S. Department of Commerce
- U.S. Department of Defense
- U.S. Department of Energy
- U.S. Department of Homeland Security
- U.S. Department of Justice
- U.S. Department of State
- U.S. Department of Transportation
- U.S. Environmental Protection Agency

SCC Members

- Agricultural Retailers Association
- American Chemistry Council
- American Forest and Paper Association
- American Petroleum Institute
- Chemical Producers and Distributors Association

- Successfully launched the Web-based Security Awareness Training Program, with over 2,100 completions to date.
- Continued information-sharing efforts to include two classified briefings for the private sector in which the Intelligence Community provided briefings on global trends regarding infrastructure.

KEY INITIATIVES

Sector partners are already implementing numerous protective programs to meet security goals. Key initiatives within the sector include the following:

- Securing high-risk facilities by implementing the Chemical Facility Anti-Terrorism Standards and ensuring compliance with the Maritime Transportation Security Act.
- Improving security practices and raising security awareness through private sector security guidance programs, documents, and/or plans.
- Enhancing information sharing through the Chemical Sector Security Summit, the Cross-Sector Cybersecurity Working Group, American Society for Industrial Security International Annual Security Conference, and the Homeland Security Information Network.
- Raising awareness by providing educational training opportunities, such as Vehicle-Borne Improvised Explosive Device training and Web-Based Chemical Security Awareness Training, for Chemical Sector security professionals and security partners.
- Expanding participation in the research and development process through the SCC Research and Development Working Group.
- Increasing cybersecurity awareness and emphasizing integration with physical security.

PATH FORWARD

Numerous steps will be taken as the Chemical Sector moves forward in securing its resources. These steps may include the following:

- Work with Congress and other security partners through DHS in an effort to make permanent the Department's regulatory authority over security at high-risk facilities.
- Work through the Critical Infrastructure Partnership Advisory Council environment to increase the number of cybersecurity points of contact through the sector and collaborate with the National Cybersecurity Division to provide cybersecurity information to the sector.

"I appreciated the time and materials and found the information very valuable."

Security Outreach and Awareness Program Participant

"Your Summit was EXCELLENT with credit to DHS!"

Chemical Sector Security Summit Participant

"The workshop gave me a better understanding of the roles DHS, State Police, FBI [U.S. Federal Bureau of Investigation], etc., play in the security/safety of the chemical arena."

Security Seminar and Exercise Series Participant

- Compressed Gas Association
- CropLife America
- Institute of Makers of Explosives
- International Institute of Ammonia Refrigeration
- International Liquid Terminals Association
- National Association of Chemical Distributors
- National Paint & Coatings Association
- National Petrochemical and Refiners Association
- Society of Chemical Manufacturers and Affiliates
- The Chlorine Institute
- The Fertilizer Institute
- The Society of the Plastics Industry, Inc.

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 planning for these facilities has 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 sector's private sector members, including commercial facility owners, operators, and trade associations, make up the Commercial Facilities Sector Coordinating Council (SCC). The sector's public sector members form the Commercial Facilities Government Coordinating Council (GCC). The U.S. Department of Homeland Security serves as the Sector-Specific Agency for the Commercial Facilities Sector.

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 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 manmade incidents.
- Institute a robust sector-wide research and development 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.

SELECTED ACCOMPLISHMENTS

Sector partners continue to maintain and Both private and public partners in the Commercial Facilities Sector have made numerous accomplishments in bolstering sector security. Some of the sctor's accomplishments over the past year include the following:

- Developed *Active Shooter – How to Respond* training materials, the *Risk Self Assessment Tool for Stadiums and Arenas*, and *Evacuation Planning Guide for Stadiums*.
- Expanded cybersecurity outreach efforts and the Cybersecurity Working Group.
- Improved information sharing through the sponsorship of security clearances for more corporate-level officials.
- Implemented emergency drills/tabletop exercises at all 31 National Football League stadiums.

KEY INITIATIVES

Private and public security partners are already engaged in numerous initiatives to help meet the Commercial Facilities Sector's security goals. These initiatives include the following:

- Improving security practices and raising security awareness through *Active Shooter – How to Respond* training materials, Building Owners and Managers Association international awareness programs, the Commercial Facilities Sector-Specific Agency outreach program, *Evacuation Planning Guide for Stadiums*, *National Football League Best Practices for Stadium Security*, and *Protective Measures Guide*.

GCC Members

- General Services Administration
- National Endowment for the Arts
- U.S. Department of Commerce
- U.S. Department of Education
- U.S. Department of Homeland Security
- U.S. Department of Housing and Urban Development
- U.S. Department of the Interior
- U.S. Department of Justice
- U.S. Environmental Protection Agency

SCC Members

- Affinia Hospitality
- BOMA International
- Dallas Convention Center
- International Association of Amusement Parks and Attractions
- International Association of Assembly Managers
- International Association of Fairs and Exhibitions

- Addressing the myriad issues constituting potential and actual threats and risks to the safety and security of fans at sporting events through the establishment of the National Center for Spectator Sports Safety and Security.
- Strengthening both the international supply chain and U.S. border security through the Customs-Trade Partnership Against Terrorism initiative.
- Providing educational training for security professionals and venue mangers through the International Association of Assembly Managers Academy for Venue Safety and Security, Protective Security Coordination Division training classes, and Shopping Center Security Terrorism Awareness Training.
- Developing the *Risk Self Assessment Tool for Stadiums and Arenas*, which offers arenas and stadiums the capability to balance resiliency with focused, risk-informed prevention, protection, and preparedness activities.
- Encouraging the development and deployment of new and innovative antiterrorism products and services by providing liability protections set forth in the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act).

PATH FORWARD

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

- Develop more subsector Protective Measures Guides comparable to the *Active Shooter – How to Respond* training manual.
- Release guides within the next year for the Lodging and Outdoor Events Subsectors.
- Fully establish and re-engage the Cybersecurity Working Group and expand cybersecurity outreach efforts.
- Continue to support the Southeast Region Research Initiative and Community and Regional Resilience Initiative program, the Bomb-Making Materials Awareness Program, and the Surveillance Detection and Protective Measures courses.

"The Milwaukee Mile racetrack made use of the Evacuation Planning Guide to prepare an evacuation plan; the plan was implemented during an inclement weather situation at the racetrack."

2009 Commercial Facilities Sector Annual Report

"The common security concern of the [Commercial Facilities] Sector is to enhance the protection of facilities and the public from all hazards without compromising accessibility and profitability."

2009 Commercial Facilities Sector Annual Report

"All 18 CIKR sectors made use of the Active Shooter materials [developed by the Commercial Facilities Sector]."

2009 Commercial Facilities Sector Annual Report

- 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
- Related Management Company
- Retail Industry Leaders Association
- Self Storage Association
- Stadium Management Association
- The Loss Prevention Foundation
- The Real Estate Roundtable
- The Walt Disney Company
- Tishman Speyer Properties
- 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 40 companies and trade associations that form the Communications Sector Coordinating Council (SCC), while seven public sector members form the Communications Government Coordinating Council (GCC). The National Communications System serves as the Sector-Specific Agency. The Government is responsible for the management of sector equities such as the National Coordinating Center (NCC) and the Network Security Information Exchange.

VISION

The Communications Sector acknowledges the Nation's critical reliance on assured communications. The Communications Sector will strive 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 security 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 the law enforcement and intelligence communities and key decisionmakers in the sector.
- Establish effective cross-sector coordination mechanisms to address critical interdependencies, including incident situational awareness and cross-sector incident management.

SELECTED ACCOMPLISHMENTS

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

- Completed the baseline Communications Sector National Risk Assessment in 2008.
- Participated in the Government's Project 12 and the White House's 60-day review of cybersecurity policies.
- Developed industry best practices that cover multiple segments and processes through the Network Reliability and Interoperability Council.

KEY INITIATIVES

The Communications Sector has protective and preparedness programs, which focus strongly on response and recovery, to help ensure the security of the communications infrastructure and delivery of services.

Key initiatives within the sector include:

- Developing more effiicient communications capabilities through the Government-to-Government Priority Telecommunications Services via the Government Emergency Telecommunications Service and National Security (NS)/Emergency Preparedness (EP) Priority Telecommunications Services.
- Establishing the Telecommunications Service Priority program, which is a regulatory, admistrative, and operational system authorizing and providing for priority treatment of telecommunications services that support NS/EP missions and that are critical to preparing for and responding to emergencies and disaster situations.
- Enhancing information sharing and increasing government situational awareness through the development and employment of the Network Security Information Exchange and Disaster Information Reporting System.

GCC Members

- Federal Communications Commission
- Federal Reserve Board
- General Services Administration
- National Association of Regulatory Utility Commissioners
- National Telecommunications and Information Administration
- U.S. Department of Agriculture
- U.S. Department of Commerce
- U.S. Department of Defense
- U.S. Department of Homeland Security
- U.S. Department of the Interior
- U.S. Department of Justice
- U.S. Department of Transportation

SCC Members

- 3U Technologies
- Alcatel-Lucent
- Americom-GS
- Association of Public Television Stations
- AT&T
- Boeing
- CTIA The Wireless Association
- Cincinnati Bell
- Cisco
- Comcast

PATH FORWARD

The sector will be working to determine the next steps in the implementation of the Communications Sector-Specific Plan, including the following:

- Continue to develop next-generation priority services to meet the evolving requirements of critical communication customers in a converged communication environment.
- Develop a Communications Sector outreach program to educate Communications Sector customers and other infrastructures on communications infrastructure resiliency and risk management practices.
- Focus on cybersecurity-related programs and activities.
- Develop points of contact in State governments to facilitate regional coordination.
- Ensure timely, relevant, and accurate threat information sharing between the law enforcement and intelligence communities and key decisionmakers in the sector.
- Implement policies to enable appropriate industry partners to get necessary security clearances.
- Develop procedures to integrate get input from industry and State and local officials into threat assessments.
- Continue to develop protocols to manage the exponential surge in calls during an emergency and ensure the integrity of sector networks during and after an emergency event.

"[The Disaster Information Reporting System] was activated for Tropical Storm Fay and for Hurricanes Gustav and Ike."

2009 Communications Sector Annual Report

"The Communications Dependency on Electric Power Working Group conducted a cross-sector dependency analysis of the Communications Sector's dependence on commercially available power sources; addressed the potential for, and recovery from, long-term outages (LTOs); and examined key cross-sector organizations, agreements, policies, and guidelines."

2009 Communications Sector Annual Report

"The expansion of the owners' and operators' membership and participation in the NCC [National Coordinating Center] has grown from 21 in 2002 to 52 companies in 2009 and contributes to increased awareness and information sharing.

2009 Communications Sector Annual Report

- Computer Sciences Corporation
- Digi International
- DirecTV
- Embarq
- Hughes Network Systems
- Internet Security Alliance
- Intrado
- Juniper Networks
- Level 3
- McLeodUSA
- Motorola
- National Association of Broadcasters
- National Cable & Telecommunications Association
- Nortel
- Qwest
- Rural Cellular Association
- The Satellite Broadcasting and Communications Association
- Satellite Industry Association
- SAVVIS
- Sprint Mobile
- Telcordia
- Telecommunications Industry Association
- TeleContinuity, Inc.
- TerreStar Networks, Inc.
- Tyco
- Utilities Telecom Council
- U.S. Internet Services Provider Association
- U.S. Telecom Association
- VeriSign
- Verizon

CRITICAL MANUFACTURING SECTOR

PARTNERSHIP

The Critical Manufacturing Sector is composed of four broad manufacturing industries: primary metal manufacturing; machinery manufacturing; electrical equipment, appliance, and component manufacturing; and transportation equipment manufacturing. In 2006, these four industries employed 1.1 million workers and manufactured products that totaled $676 billion. The Sector Coordinating Council (SCC) currently includes representatives from 10 manufacturing companies and is exploring the addition of recognized trade associations. The U.S. Department of Homeland Security (DHS) is the Sector-Specific Agency (SSA), and chair of the Government Coordinating Council (GCC).

GOALS

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

- Achieve an understanding of the assets, systems, and networks that comprise the critical infrastructure of the Critical Manufacturing Sector.
- Develop an up-to-date risk profile of the assets, systems, and networks within the Critical Manufacturing Sector that will enable a risk-based prioritization of protection activities.
- Develop protective programs and resiliency strategies that address the risk to the Critical Manufacturing Sector without hindering its economic viability.
- Create a means of measuring the progress and effectiveness of Critical Manufacturing Sector critical infrastructure and key resources (CIKR) protection activities.
- Develop processes for ensuring appropriate and timely information sharing between government and private sector stakeholders in the Critical Manufacturing Sector.

SELECTED ACCOMPLISHMENTS

Sector partners have taken initial measures to becoming a more secure and resilient sector, including the following:

- Established DHS as the Critical Manufacturing SSA.
- Formed the Critical Manufacturing GCC.
- Developed the Critical Manufacturing Sector-Specific Plan.
- Fostered partnerships through information sharing.
- Collaborated with the Defense Industrial Base Sector to assess risk posed to certain manufacturing facilities.

KEY INITIATIVES

Sector partners, both public and private, engage in a wide variety of activities to mitigate risk. These activities will enable the sector to further enhance its security posture.

Key initiatives within the sector include:

- Implementing the National Infrastructure Protection Plan Sector Partnership Model that provides the framework for the SSA to collaborate and coordinate with members of the Critical Manufacturing SCC and Critical Manufacturing GCC on a variety of projects.
- Obtaining DHS sponsorship of security clearances for Critical Manufacturing Sector partners to ensure timely distribution of information potentially critical to the security of private sector owners and operators.
- Participating in the Enhanced Critical Infrastructure Protection Initiative that allows DHS Protective Security Advisors to form partnerships with the owners and operators of the Nation's high-priority CIKR.
- Increasing information sharing by using the Homeland Security Information Network Critical Sectors (HSIN-CS).

GCC Members

- U.S. Department of Commerce
- U.S. Department of Defense
- U.S. Department of Energy
- U.S. Department of Homeland Security
- U.S. Department of Justice
- U.S. Department of Labor
- U.S. Department of State
- U.S. Department of Transportation
- U.S. Department of the Treasury
- U.S. Environmental Protection Agency
- U.S. Small Business Administration

PATH FORWARD

The sector has a variety of ongoing and planned activities to increase the protection and resiliency of the sector in the coming year. Some of these activities include the following:

- Develop a workshop to identify mission needs for research and development, as well as modeling, simulation, and analysis.
- Develop a workshop to discuss the sharing of classified and unclassified information relevant to Critical Manufacturing Sector security.
- Develop a workshop to address previously identified gaps in information sharing between public and private Critical Manufacturing Sector partners.
- Develop an information-sharing platform through the HSIN-CS portal.
- Increase the involvement of State and local communities.
- Regionalize the SCC.

"Sector assets are highly dispersed worldwide, creating dependency on a complex and interconnected global supply chain."

2009 Critical Manufacturing Sector Annual Report

"The Critical Manufacturing Sector participated in the DHS Critical Foreign Dependencies Initiative – an effort to identify foreign-based infrastructure that could significantly affect the domestic Critical Manufacturing Sector if disrupted."

2009 Critical Manufacturing Sector Annual Report

"To address the key issue of cybersecurity, the CMSCC formed a Cyber Working Group with cybersecurity subject matter expert representatives from its member companies."

2009 Critical Manufacturing Sector Annual Report

SCC Members

- ArcelorMittal USA
- Caterpillar Inc.
- Chrysler LLC
- Deere & Company
- Ford Motor Company
- General Motors
- Goodyear Tire & Rubber Company
- Kohler Company
- Navistar International Corporation
- U.S. Steel Corporation

DAMS SECTOR

PARTNERSHIP

The Dams Sector comprises dam projects, navigation locks, levees, hurricane barriers, mine tailings impoundments, and other similar water retention and/or control facilities. Dams are vital to the Nation's infrastructure and provide a wide range of economic, environmental, and social benefits, including hydroelectric power, river navigation, water supply, flood control, and recreation. There are over 82,000 dams in the United States; approximately 65% are privately owned and more than 85% are regulated by State dam safety offices.

The Dams Sector operates under the auspices of the Critical Infrastructure Partnership Advisory Council (CIPAC) framework, which facilitates effective coordination between Federal infrastructure protection programs and infrastructure protection activities of State, local, tribal, and territorial governments, and the private sector. The CIPAC framework consists of a Sector Coordinating Council (SCC) and Government Coordinating Council (GCC). The Dams SCC is composed of non-Federal owners and operators as well as trade associations, and serves as the private sector interface with the Federal Government on issues related to the security of dams, locks, and levees. The Dams Sector GCC acts as the government counterpart and partner to the SCC to plan, implement, and execute sector-wide security programs for the sector's assets. It comprises representatives from across various levels of government (Federal, State, local, and tribal), including Federal owners and operators, and State and Federal regulators of sector assets. The Office of Infrastructure Protection within the U.S. Department of Homeland Security, as the Dams Sector-Specific Agency, serves as the GCC Chair.

VISION

The Dams Sector will identify the measures, strategies, and policies appropriate to protect its assets from terrorist acts and enhance their capability to respond to and recover from attacks, natural disasters, or other emergencies through the development of multifaceted, multilevel, and flexible protective programs and resiliency strategies 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 the 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 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.

SELECTED ACCOMPLISHMENTS

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

- Demonstrated sector maturation by forming the Levee Subsector Coordinating Council (LSCC) and the State Dam Security Panel.
- Conducted a series of exercises with government- and privately-owned dams along the same river basin to test communication and interoperability capabilities.
- Identified and characterized the subset of high-consequence facilities within the Dams Sector through the implementation of the Consequence-Based Top-Screen methodology.
- Developed a number of reference documents focused on security awareness, protective measures, and crisis management.

GCC Members

- Bonneville Power Administration
- Federal Energy Regulatory Commission
- International Boundary and Water 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
- U.S. Department of Agriculture, Natural Resources Conservation Service
- U.S. Department of Commerce, National Weather Service
- U.S. Department of Defense, U.S. Army Corps of Engineers
- U.S. Department of Energy
- U.S. Department of Homeland Security, Federal Emergency Management Agency
- U.S. Department of Homeland Security, Office of Infrastructure Protection (SSA)
- U.S. Department of Homeland Security, Science and Technology Directorate
- U.S. Department of Homeland Security, U.S. Coast Guard
- U.S. Department of Labor, Mine Safety and Health Administration
- U.S. Department of State
- U.S. Department of the Interior, U.S. Bureau of Reclamation
- U.S. Environmental Protection Agency

- Addressed research and development gaps through experimental and numerical studies.
- Conducted the first annual National Dam Security Forum.

KEY INITIATIVES

The Dams Sector has a number of initiatives to enhance the prevention, protection, security, and resiliency of the Nation's dams, levees, and locks. Some of these initiatives include the following:

- Developing improved blast-induced damage analysis capabilities and simplified damage estimation models for dams, locks, and levees.
- Improving the sector's capability to predict the extent of damage and develop mitigation measures for waterside attack scenarios.
- Identifying and characterizing critical infrastructure.
- Assessing the economic and loss-of-life consequences of dam failures.
- Determining the status of State-level dam security and protection jurisdictional programs.
- Improving regional resilience and preparedness through an annual series of exercises.
- Developing and widely distributing technical reference handbooks, guides, brochures, and training materials for dam and levee owners and operators.

PATH FORWARD

The Dams Sector will seek progression in three areas: information-sharing obstacles, funding constraints, and infrastructure condition. This progress will be achieved by taking the following steps:

- Continue to investigate more efficient mechanisms to share information with the sector's international partners.
- Continue to share information with sector partners via the Homeland Security Information Network – Critical Sectors Dams Portal and other channels.
- Continue to identify and characterize critical assets to demonstrate the need for a risk-based, multiyear, multijurisdictional program.

"The State Dam Security Panel first annual National Dam Security Forum was held in September 2008 in conjunction with the annual Association of State Dam Safety Officials Dam Safety Conference."

2009 Dams Sector Annual Report

"[Consequence-Based Top Screening] was implemented as a collaborative effort within the Critical Infrastructure Partnership Advisory Council (CIPAC) framework and is supported by a user-friendly Web-based tool that allows users to submit consequence data."

2009 Dams Sector Annual Report

"The aging of the country's dams, levees, and major waterway navigation structures continues to be a threat to the sector and a factor in its risk profile."

2009 Dams Sector Annual Report

"Recognizing the need to plan, coordinate, and focus ongoing efforts, sector partners began developing a comprehensive 'Roadmap to Secure Control Systems in the Dams Sector."

2009 Dams Sector Annual Report

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 Public Utility District #1
- Consumers Energy
- Colorado River Energy Distribution Association
- Dominion Resources
- Duke Energy Corporation
- Exelon Corporation
- Hydro-Québec
- National Association of Flood & Stormwater Management Agencies
- National Hydropower Association
- National Mining Association
- National Water Resources 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 Santee Cooper
- Southern California Edison
- Southern Company Generation
- United States Society of Dams
- Xcel Energy Corporation

LSCC Members

- Association of State Floodplain Managers
- Los Angeles County Department of Public Works
- Metropolitan Water District of Southern California
- National Association of Flood and Stormwater Management Agencies
- South Lafourche Levee District

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, DoD leads a collaborative, coordinated effort to identify, assess, and improve risk management of critical infrastructure within the sector. Members of defense industry associations and DIB private sector critical infrastructure and key resources (CIKR) owners and operators form the DIB Sector Coordinating Council (SCC). The DIB Sector Government Coordinating Council (GCC) is composed of members from the U.S. Department of Homeland Security (DHS), DoD, the U.S. Department of the Treasury, the U.S. Department of Commerce, and the U.S. Department of Justice.

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

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

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.

Information Security: Manage risk to information that identifies or describes characteristics or capabilities of a critical DIB asset, or by the nature of the information would represent a substantial risk or adverse impact to the CIKR or the DIB asset.

SELECTED ACCOMPLISHMENTS

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

- Revised the sector's Important Capabilities List and Critical Asset List.
- Completed 31 awareness visits and 21 on-site assessments.
- Completed initial deployment of the DIBNet secure information-sharing system and expanded the DoD DIB Cyber Security/Information Assurance (DIBCS/IA) pilot program.
- The SCC adopted the Defense Security Information Exchange to support private sector cybersecurity activities.
- Developed the *DIB Pandemic Influenza Guidebook* and Webinar.

KEY INITIATIVES

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

Key initiatives within the sector include:

- Developing, coordinating, and approving the annual listing of DIB CIKR and notifying asset owners and operators of changes in criticality.

GCC Members

- U.S. Department of Commerce
- U.S. Department of Defense
- U.S. Department of Homeland Security
- U.S. Department of Justice
- U.S. Department of State
- U.S. Department of the Treasury

SCC Members

- AAI Corporation
- Aerospace Industries Association
- Alliant Techsystems
- ASIS International
- BAE Systems
- Boeing Company
- Booz Allen Hamilton
- Computer Sciences Corporation

- Developing and deploying a risk self-assessment tool (SAT).
- Establishing and employing business continuity plans for CIKR owner and operator assets.
- Participating in exercises to enhance emergency preparedness.
- Identifying local dependencies and conducting dependency analyses.
- Maintaining and distributing the *Defense Critical Infrastructure Program Resilience Guide* and other best practices materials.

PATH FORWARD

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

- Implement actions in the areas of development of an SAT, interdependency identification, information sharing, DIB criticality, security classification, cyber and physical security policy, and information assurance.
- Continue to advocate for a better understanding of mission consequence issues within DHS and among CIKR partners throughout the DIB as well as the other sectors.

"The DIB SCC maintains its Emergency Contact Listing that allows CIKR owners and operators [and defense industry associations] to participate in DHS-sponsored emergency planning, response, and recovery meetings."

2009 Defense Industrial Base Sector Annual Report

"In response to the growing cybersecurity threats and reported incidents within the DIB Sector, the Deputy Secretary of Defense directed the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer (NII/DoD CIO) to establish the DIB Cyber Security/ Information Assurance (DIBCS/IA) Task Force."

2009 Defense Industrial Base Sector Annual Report

"The DIB SCC has adopted the Defense Security Information Exchange (DSIE)… as its Information/Cyber Security Standing Committee…. The DSIE has 28 member companies and more than [150] US CERT [United States Computer Emergency Readiness Team] portal users [that routinely share cyber security alerts and remediation actions]."

2009 Defense Industrial Base Sector Annual Report

- Defense Security Information Exchange
- General Atomics
- General Dynamics
- General Electric
- Honeywell
- Industrial Security Working Group
- L-3 Communications
- Lockheed Martin Corporation
- MITRE
- National Classification Management Society
- National Defense Industrial Association
- Northrop Grumman Corporation
- Orbital Sciences
- Pratt & Whitney (UTC)
- Raytheon Company
- Rockwell Collins
- Rolls Royce
- Science Applications International Corporation

EMERGENCY SERVICES SECTOR

PARTNERSHIP

The Emergency Services Sector (ESS) is a system of prevention, protection, preparedness, response, and recovery elements that forms the Nation's first line of defense for preventing and mitigating risk. The ESS encompasses a wide range of emergency response functions, with the primary mission to save lives, protect property and the environment, assist communities impacted by disasters (natural or malevolent), and aid recovery from emergency situations. For the ESS, the owners and operators represent multiple distinct disciplines and systems that inherently reside in the public safety arena within State and local government agencies but which also include disciplines that are private, for-profit businesses.

The U.S. Department of Homeland Security (DHS) is the Sector-Specific Agency (SSA) for the ESS and delegates its SSA duties to the Office of Infrastructure Protection (IP). As the SSA, IP has numerous responsibilities including leading, integrating, and coordinating the overall national effort to enhance ESS critical infrastructure and key resources (CIKR) protection. The Emergency Services Government Coordinating Council (GCC), chaired by DHS, consists of Federal departments and agencies integral to the sector and assists in the coordination of CIKR strategies and activities, policy, and communication within their organizations, across government, and between governments and sector members. The Emergency Services Sector Coordinating Council (SCC) is a self-organized, self-led body of ESS members who work collaboratively with the SSA and GCC. The Emergency Services SCC is organized through professional associations that represent the five emergency service disciplines: Fire Emergency Services, Law Enforcement, Emergency Medical Services, Emergency Management, and Public Works. The Emergency Services SCC provides DHS with a reliable and efficient way to communicate and consult with the sector on protective programs and issues.

VISION

An Emergency Services Sector in which facilities, key support systems, information and coordination systems, and personnel are protected from both ordinary operational risks and from extraordinary risks or attacks, ensuring timely, coordinated all-hazards emergency response and public confidence of the citizens who depend on the sector to protect their lives and property.

GOALS

The SSA collaborates with sector partners to create goals that represent the sector's view of how to achieve a secure, protected, and resilient ESS. The following goals underline the sector's emphasis on protecting the human and physical assets of the sector:

- Partnership Engagement: To build a partnership model that will enable the sector to effectively sustain a collaborative planning and decisionmaking culture.
- Situational Awareness: To build an information-sharing environment that ensures the availability and flow of accurate, timely, and relevant information and/or intelligence about terrorist threats and other hazards, information analysis, and incident reporting.
- Prevention, Preparedness, and Protection: To employ a risk-based approach to developing protective efforts designed to improve the overall posture of the sector through targeted risk management decisions and initiatives.
- Sustainability, Resiliency, and Reconstitution: To improve the sustainability and resiliency of the sector and increase the speed and efficiency of restoration of normal services, levels of security, and economic activity following an incident.

SELECTED ACCOMPLISHMENTS

Some of the sector's key accomplishments for the past year include the following:

- Realigned and strengthened sector goals to support an engaged and well-informed sector community that takes responsibility for its own safety and sustainability.
- Expanded the sector's list of critical infrastructure.
- Established practitioner-based working groups.
- Designed and distributed a brochure directed at emergency responders to raise their level of awareness regarding the need to develop protective measures for themselves and their families.
- Developed and distributed an educational and outreach guide for commercial facility employees and operators, used as training guidance for response to an "active shooter" event.
- Developed a Web-based CIKR resource center for the sector.
- Conducted Webinars on the *Pandemic Influenza Guide for Critical Infrastructure and Key Resources.*

GCC Members

- American Red Cross
- Federal Bureau of Investigation
- Federal Emergency Management Agency
- Immigration and Customs Enforcement
- National Guard Bureau
- Office of Bombing Prevention
- Office of Cybersecurity and Communications
- Office of Health Affairs
- Office of Infrastructure Protection
- Office of State and Local Law Enforcement
- Science and Technology
- State, Local, Tribal, Territorial Government Coordinating Council
- Transportation Security Administration
- U.S. Coast Guard
- U.S. Department of Agriculture Forest Service
- U.S. Department of Health and Human Services
- U.S. Department of Justice
- U.S. Department of Transportation
- U.S. Environmental Protection Agency
- U.S. Fire Administration
- U.S. Secret Service

KEY INITIATIVES

Initiatives within the sector range from measures to prevent, deter, and mitigate threats to timely, effective response and restoration following terrorist attacks, natural disaster, or other incidents. Key initiatives within the sector include:

- Assisting jurisdictions in developing detailed plans to address improvised explosive device security threats.
- Establishing an all-hazards framework and national priorities through the *National Preparedness Guidelines and Target Capabilities List*.
- Employing the Homeland Security Information Network and ESS-relevant portals to share and disseminate sensitive information regarding alerts, warnings, suspicious activity reporting, and intelligence and analysis products.
- Collaborating with the Pacific Northwest Economic Region, the U.S. Army Corps of Engineers, and Pacific Northwest Region CIKR partners to develop and conduct a series of exercises along the Columbia River Basin in 2009.
- Identifying protective measures, informing facility owners and operators, and establishing and enhancing relationships through the Enhanced Critical Infrastructure Protection initiative.
- Establishing a pilot project to use visualization platforms to create a national model for interstate information sharing.

PATH FORWARD

Numerous steps will be taken to address challenges facing the sector, including the following:

- Enhance clarity of the ESS role in critical infrastructure protection that articulates the sector's CIKR mission and related activities and acknowledges the direct correlation between protection of the sector and protection of the public.
- Improve consistency in coordination among DHS and other Federal agencies' programs and messages that apply to ESS.
- Develop a truly collaborative process that supports realistic and sustainable efforts to protect the Nation's critical infrastructure.
- Develop actionable products for emergency services personnel reflective of their needs.
- Continue to reach out and build relationships with Federal, State, local, tribal, and territorial CIKR partners to ensure effective coordination of activities among all government agencies and within the IP that impact emergency responders.
- Continue to collaborate with the SCC to facilitate appropriate, value-added exercise objectives for the sector.

"The International Association of Fire Chiefs and the Pipeline and Hazardous Materials Safety Administration (U.S. Department of Transportation) initiated efforts to establish the first Web-based National Hazardous Materials Fusion Center."

2009 Emergency Services Sector Annual Report

"The partnership model from a private sector frame of reference is the protection of 'goods and services,' whereas in ES, 'goods and services' is defined as saving lives and property. The ESS is a system of prevention, protection, preparedness, response, and recovery elements that forms the Nation's first line of defense for preventing and mitigating risk. Therefore, the partnership activities and programs appropriate to the sector are those that allow for an inward-focused perspective, as well as maintaining the ability of the response community to engage in its mission during an all-hazard event."

2009 Emergency Services Sector Annual Report

Emergency Services Sector Disciplines

- Law Enforcement
- Fire Emergency Services
- Emergency Management
- Emergency Medical Services
- Public Works

SCC Members

- American Ambulance Association
- American Public Works Association
- International Association of Chiefs of Police
- International Association of Emergency Managers
- International Association of Fire Chiefs
- National Association of Security Companies
- National Association of State EMS Officials
- National Association of State Fire Marshalls
- National Emergency Management Association
- National Native American Law Enforcement Association
- National Sheriffs' Association
- Security Industry 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 that is owned, operated, hosted, and regulated by numerous 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 the Oil and Natural Gas Sector Coordinating Councils (SCCs), and public sector security partners comprise 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 the oil and natural gas industry. The U.S. Department of Energy serves as the Sector-Specific Agency of the Energy Sector.

VISION

The Energy Sector envisions 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 business continuity 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; 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.

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:

- Developed several additional reliability standards for the power grid, which have been approved by the Federal Energy Regulatory Commission.
- Initiated enhanced approaches to plan for and counter cybersecurity threats to energy infrastructure operations.
- Worked very closely with the Chemical Sector to implement new rules regarding safety and security at chemicals facilities, many of which are also energy-related facilities and infrastructure.
- Established a working group under the Critical Infrastructure Partnership Advisory Council to develop sector-specific approaches to metrics in order to better track and report on sector security advances.
- Developed an Oil and Natural Gas SCC Emergency Response Working Group and hosted several cross-sector emergency management workshops, which: aim to promote an integrated private sector and government response during natural disasters and terrorist incidents; and specifically to identify access solutions to chemical facilities impacted by such incidents.

GCC Members

- Federal Energy Regulatory Commission
- National Association of Regulatory Utility Commissioners
- National Association of State Energy Officials
- U.S. Department of Agriculture
- U.S. Department of Defense
- U.S. Department of Energy
- U.S. Department of Homeland Security
- U.S. Department of State
- U.S. Department of the Interior
- U.S. Department of Transportation
- U.S. 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 Independent System Operator
- Reliability First Corporation
- Southern Company Services, Inc.

KEY INITIATIVES

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

Key initiatives within the sector include the following:

- Examining potential systemwide energy resiliency issues.
- Responding to Chemical Facility Anti-terrorism Standards requirements that impact energy assets.
- Drafting metrics in cooperation with the Oil and Natural Gas SCC and GCC Joint Energy Metrics Working Group.
- Implementing North American Electric Reliability Corporation standards for physical and cybersecurity in the electric sector.
- Expanding education, training, and outreach.
- Refining incident management planning and response by applying lessons learned.

PATH FORWARD

While significant progress has been made in securing the energy infrastructure, challenges remain, including data collection costs and information protection, communication of interdependencies and the value of partnerships to owners and operators, and development of national cybersecurity strategies. The Energy Sector will take numerous steps to move forward to address these challenges, including the following.

- Build and strengthen existing critical infrastructure and key resources protection partnerships.
- Facilitate communication and information exchange through the Homeland Security Information Network, the Infrastructure Security & Energy Restoration Internet Network, training and exercises, energy situation reports, and the National Infrastructure Protection Plan partnership framework.
- Continue to work with other sectors to understand interdependencies.
- Improve energy security through critical infrastructure partnerships beyond national borders.
- Continue to encourage sector participation in U.S. Department of Homeland Security Web-based training opportunities and voluntary cooperation within energy subsectors through their trade organizations.

"More than 5.5 of 6.5 million barrels per day (MMBD) of Gulf Coast refining capacity had been restored four weeks after Hurricane Rita's landfall."

2009 Energy Sector Annual Report

"Electricity Subsector owners and operators are working with the Federal Emergency Management Agency (FEMA) and state and local emergency agencies to ensure critical utility personnel are appropriately prioritized during a pandemic emergency."

2009 Energy Sector Annual Report

"The purpose of Smart Grid is the modernization of the electric grid in order to enhance security and the reliability of the energy infrastructure. These investments should reduce the frequency and scope of power outages through a more intelligent two-way control and communications system."

2009 Energy Sector Annual Report

Oil and Natural Gas SCC Members

- American Exploration & Production Council
- American Gas Association
- American Petroleum Institute
- American Public Gas Association
- Association of Oil Pipe Lines
- Canadian Association of Petroleum Producers
- Canadian Energy Pipeline Association
- Energy Security Council
- Gas Processors Association
- Independent Petroleum Association of America
- International Association of Drilling Contractors
- International Liquid Terminals Association
- Interstate Natural Gas Association of America
- National Association of Convenience Stores
- National Ocean Industries Association
- National Petrochemical & Refiners Association
- National Propane Gas Association
- Offshore Marine Service Association
- Offshore Operators Committee
- Petroleum Marketers Association of America
- Society of Independent Gas Marketers Association
- U.S. Oil & Gas Association
- Western States Petroleum Association

FOOD AND AGRICULTURE SECTOR

PARTNERSHIP

The Food and Agriculture Sector is composed of complex production, processing, and delivery systems that encompass more than two million farms, approximately 900,000 firms, and 1.1 million facilities; as a whole, it accounts for roughly one-fifth of the Nation's economic activity. 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, territorial and local agricultural, public health, 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 U.S. Food and Drug Administration (FDA).

VISION

The Food and Agriculture Sector strives to ensure that the Nation's food and agriculture networks and systems are secure, resilient, and rapidly restored after all-hazards incidents. Public and private partners aim to reduce vulnerabilities and minimize consequences through risk-based decisionmaking and effective communication.

GOALS

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

- Work with State and local entities to ensure that they are prepared to respond to incidents.
- Improve sector analytical methods to enhance and validate detection of a wide spectrum of threats.
- Improve sector situational awareness through enhanced intelligence communication and information sharing.
- Tailor risk- and performance-based protection measures to the sector's physical and cyber assets, personnel, and customers' products.
- Address response and recovery at the sector level, not just as separate enterprises.
- Expand laboratory systems and qualified personnel.

SELECTED ACCOMPLISHMENTS

The Food and Agriculture Sector had many accomplishments during the past year, including the following:

- Developed a new sector vision statement.
- Implemented the Food and Agriculture Sector Criticality Assessment Tool (FAS-CAT) to help identify critical assets in the sector and provide reporting mechanisms to DHS.
- Increased sector communications and the Homeland Security Information Network (HSIN), to include a metric defining the success of HSIN.
- Conducted the Federal Emergency Management Agency (FEMA) Region VI Food and Agriculture Regional Exercise (FARE) on February 4–5, 2009, at the Memorial Institute for the Prevention of Terrorism (MIPT) in Oklahoma City, Oklahoma.
- Created a working group to rewrite the original 2007 Sector-Specific Plan (SSP) and 2008 SSP Update to reflect a unified Federal Government approach.

KEY INITIATIVES

The sector has a number of important initiatives under way to ensure that the Nation's food and agriculture networks and systems are secure, resilient, and rapidly restored after all-hazards incidents.

Key initiatives within the sector include the following:

- Implementing several surveillance programs, including the Pre-harvest Surveillance Program for Animal and Plant Pathogens Initiative and the Post-harvest (Food) Surveillance for Biological and Chemical Agents Initiative.
- Promoting educational training through programs such as the Food and Agriculture Response and Recovery Exercises.
- Developing and distributing food and agriculture defense training and awareness materials.
- Conducting research through the Pre-harvest Research and Development

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
- Intertribal Agricultural Council
- National Assembly of State Chief Livestock Health Officials
- National Association of County and City Health Officials
- National Association of State Departments of Agriculture
- National Environmental Health Association
- National Oceanic and Atmospheric Agency
- State, Local, Territorial, and Tribal Government Coordinating Council
- The National Plant Board
- The Navajo Nation
- U.S. Department of Agriculture
- U.S. Department of Commerce
- U.S. Department of Defense
- U.S. Department of Health and Human Services, Food and Drug Administration
- U.S. Department of Homeland Security
- U.S. Department of the Interior
- U.S. Department of Justice
- U.S. Environmental Protection Agency

Initiative and the Post-harvest (Food) Research and Development for Biological and Chemical Agents Initiative.

- Conducting risk assessments for both pre-harvest and post-harvest (food).
- Maintaining strong laboratory networks.
- Developing countermeasures for Emergency Response to a Food Contamination or an Animal Health Event.
- Implementing Recovery Assistance Development programs.
- Developing information-sharing protocols and procedures.
- Assisting owners and operators in planning and preparedness.

PATH FORWARD

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

- Increase sector membership and encourage more active participation from current members.
- Create a more effective and efficient information-sharing environment, which includes HSIN, within the sector.
- Create a three-year exercise schedule, planning for one large multi-agency exercise per year.
- Continue to work on developing and raising sector partners' awareness of the HSIN and FAS-CAT.

"USDA had designated April as its Cyber Security Awareness Month. The 3rd Annual Security Awareness Expo was held April 22–23, 2009."

2009 Food and Agriculture Sector Annual Report

"The [Foreign Animal Disease Threat] subcommittee is co-chaired by the USDA Agricultural Research Service (ARS) and the DHS Directorate for Science and Technology (S&T) and brings together subject matter experts and decision makers from eight Federal agencies to enhance interagency cooperation and collaboration to identify knowledge gaps, priorities, and budget initiatives for Federal FAD programs."

2009 Food and Agriculture Sector Annual Report

"Many sector assets defy traditional security practices because they are not "brick and mortar" entities, like buildings, bridges, or dams. Instead, they are open areas (i.e., farms, ranches, or livestock transport areas) and complex systems that span the globe."

2009 Food and Agriculture Sector Annual Report

"Although food products are regulated at the Federal level by the FDA and the USDA, most inspections, food samples, and enforcement actions are performed by State and local agencies."

2009 Food and Agriculture Sector Annual Report

SCC Members

- Agricultural Retailers Association
- American Farm Bureau Federation
- American Frozen Food Institute
- American Meat Institute
- CF Industries, Inc.
- CropLife America
- Food Marketing Institute
- Food Processors Association
- Grocery Manufacturers 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 Federal, State, local, tribal, and Territorial assets and associated elements located around the world. 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 encompasses elements associated with and often contained or housed within a government facility. The GFS also includes the Education Facilities Subsector, which covers all public and private K-12 schools; both public and private institutions of higher education; 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.

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.

SELECTED ACCOMPLISHMENTS

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

- Established seven key risk mitigation activities that target security programs that are comprehensive, coordinated, and measurable.
- Established stronger relationships with the R&D community, specifically through the DHS Directorate for S&T, to leverage new technologies to enhance security.
- Informed building occupants, employees, and security partners about the dangers of cyber threats and their potential impact on the sector.
- Maintained response readiness through a near 100 percent update and alignment of emergency plans to threat scenarios.

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 continuity of operations. These programs have contributed to a more secure sector.

Key initiatives within the sector include the following:

- Conducting building security assessments periodically according to a schedule based upon each building's Facility Security Level.
- Promoting awareness and implementation of Interagency Security Committee policies, guidelines, and best practices.
- Maintaining and/or revising Occupant Emergency Plans that can reduce the threat to personnel, property, and other assets while minimizing work disruption.
- Conducting thorough and efficient background investigations on contract guards by undertaking a suitability review and background investigation using the Office of Personnel Management e-QIP processes.
- Determining whether Federal facilities are in compliance with a range of physical security standards through countermeasure effectiveness evaluation.
- Informing, educating, and enlisting tenant agency support for monitoring suspicious activities by conducting crime prevention training seminars.
- Developing continuity plans and programs and establishing positions of priority associated with mission-essential functions.
- Promoting awareness of National Institute of Standards and Technology (NIST) Special Publication 800-53 standards and guidelines for the specification of security controls, and NIST Special Publication 800-53A for the assessment of security control effectiveness.

GCC Members

- American Society of Mechanical Engineers
- Architect of the Capitol
- Carnegie Mellon University
- Federal Aviation Administration
- Federal Facilities Administration
- General Services Administration
- Interagency Security Committee
- National Air and Space Administration
- National Archives and Records Administration
- National Center for State Courts
- National Institute of Standards and Technology
- Office of Personnel Management
- Social Security Administration

PATH FORWARD

Numerous steps will be taken as the Government Facilities Sector addresses challenges to success, including the following:

- Enhance information technology (IT) systems and related operation to include systems and technologies for the MegaCenters, Risk Assessment and Management Program, and other IT infrastructure, including database integration.
- Continue to manage communications with internal and external security partners, as well as implement design and change management strategies to ensure security partners are aware of and embrace changes in FPS mission, organization, and processes consistent with the GFS Sector-Specific Plan.
- Expand the available metrics to measure progress toward achieving the security goals of the sector.
- Redevelop the FPS risk assessment program.

"[T]he size and breadth of the GFS mean that its assets, systems, networks, and functions can be found in all corners of the globe, rendering them susceptible to the full range of natural hazards."

2009 Government Facilities Sector Annual Report

"A historical examination of terrorist attacks in modern times shows the GFS to be the most frequently attacked of all 18 CIKR sectors."

2009 Government Facilities Sector Annual Report

"The Interagency Security Council released "Facility Security Level Determinations for Federal Facilities" which provides an updated method for categorizing Federal facilities and replaces the building security level standard established in 1995."

2009 Government Facilities Sector Annual Report

Highlights of the 2009 Education Facilities Subsector Annual Report

- Expanded emergency management support to another component of the subsector, by implementing the new discretionary grant program for Higher Education Institutions, which includes training.
- Published an "Action Guide for Higher Education Emergency Management" and a "Guide to School Vulnerability Assessments."
- Collaborated with partners to provide guidance and information to the subsector on topical issues during steady state and crisis.

- U.S. Capitol Police
- U.S. Department of Agriculture
- U.S. Department of Commerce
- U.S. Department of Defense
- U.S. Department of Education
- U.S. Department of Homeland Security
- U.S. Department of Justice
- U.S. Department of Labor
- U.S. Department of State
- U.S. Department of the Interior
- U.S. Department of the Treasury
- U.S. Department of Veterans Affairs
- U.S. Environmental Protection Agency

HEALTHCARE AND PUBLIC HEALTH SECTOR

PARTNERSHIP

The Healthcare and Public Health (HPH) Sector constitutes approximately 16 percent ($2 trillion) of the gross national product 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 make up the HPH Sector Coordinating Council (SCC), while the public sector members of the partnership make 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.

VISION

The HPH Sector will achieve overall resiliency against all hazards. It will prevent or minimize damage to, or destruction of, the Nation's healthcare and public health infrastructure. It will strive to protect its workforce and preserve its ability to mount timely and effective responses, without disruption to services in non-impacted areas, and its ability to recover from both routine and emergency situations.

GOALS

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

Service Continuity: Maintain the ability to provide essential health services during and after disasters or disruptions in the availability of supplies or supporting services (e.g., water, power).

Workforce Protection: Protect the sector's workforce from the harmful consequences of all hazards that may compromise their health and safety and limit their ability to carry out their responsibilities.

Physical Asset Protection: Mitigate the risk posed by all hazards to the sector's physical assets.

Cybersecurity: Mitigate risks to the sector's cyber assets that may result in disruption to or denial of health services.

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 participation in RxResponse from 3 states to 21 states and 2 metropolitan statistical areas (MSAs) to support the medical supply chain during emergencies.
- Increased by 30 percent the number of MSAs that meet Cities Readiness Initiative criteria for effectively distributing medical countermeasures.
- Doubled the number of security site audits at medical countermeasure facilities.
- Launched the Information Sharing Workgroup and Private Sector Liaison Officer Program.
- Expanded and relaunched the Homeland Security Information Network (HSIN) portal.

KEY INITIATIVES

The HPH Sector conducts numerous activities to improve its ability to maintain service continuity and to mitigate risks to its workforce, physical assets, and cyber systems.

Key initiatives within the sector include the following:

- Improving the ability to deliver healthcare during and immediately following all-hazards events through the HHS Hospital Preparedness Program; the Joint Commission Healthcare Facility Accreditation programs; RxResponse initiative; Centers for Disease Control and Prevention (CDC) Public Health Emergency Preparedness Program; Project Public Health Ready Program; and the Drug, Biological Product, and Medical Device Shortage programs of the Food and Drug Administration.
- Enhancing workforce protection through CDC's disease detection and investigation activities and Cities Readiness Initiative.
- Protecting physical assets through the CDC Select Agent Program, Protection Office of the HHS Biomedical Advanced Research and Development Authority Program and hospital protection activities.

GCC Members

- Association of Public Health Laboratories
- Association of State and Territorial Health Officials
- National Association of County and City Health Officials
- National Indian Health Board
- U.S. Department of Agriculture
- U.S. Department of Defense
- U.S. Department of Energy
- U.S. Department of Health and Human Services
- U.S. Department of Homeland Security
- U.S. Department of Interior
- U.S. Department of Labor
- U.S. Department of Veterans Affairs

SCC Members

- American Academy of Pediatrics
- 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

- Mitigating risks associated with cybersecurity threats through the Nationwide Privacy and Security Framework, the Health Information Technology Standards Panel, the National Institute of Standards and Technology Health Information Exchange Standards, the Integrating the Healthcare Enterprise initiative, and guidance for protecting medical devices containing off-the-shelf software.

PATH FORWARD

The HPH Sector faces challenges in information sharing, sector asset prioritization, and resource allocation. The sector will continue to address these challenges by taking the following steps:

- Examine the organization of information on HSIN and the development of new, targeted information products for the sector through the joint Information Sharing Working Group.
- Participate directly in the adjudication of sector assets for the Tier 1/Tier 2 process.
- Continue to gather data regarding the effectiveness of sector critical infrastructure protection efforts to assist in resource allocation decisions.

"During Hurricanes Gustav, Hannah, and Ike, the SSA maintained regular contact with SCC and GCC members to disseminate information related to the response."

2009 Healthcare and Public Health Sector Annual Report

"[T]he rapid deployment of [health information] technologies is increasing the vulnerability of healthcare networks, systems, and data, and the consequences of cyber attacks that exploit these vulnerabilities."

2009 Healthcare and Public Health Sector Annual Report

"Health information technology received $19 billion from the [American Recovery and Reinvestment] Act, creating both the opportunity to accelerate the implementation of cyber systems within the sector as well as the challenge of protecting those systems from attack."

2009 Healthcare and Public Health Sector Annual Report

"[T]he report Federal Guidance on Antiviral Drug Use During an Influenza Pandemic, released in December 2008, provided recommendations related to antiviral prophylaxis for healthcare workers during a pandemic."

2009 Healthcare and Public Health Sector Annual Report

- America's Health Insurance Plans
- Association of Healthcare Resource and Materials Management Professionals
- Biotechnology Industry Organization
- Blue Shield of California
- Blu-Med Response Systems
- Brooklawn Memorial Park
- Health Information and Management Systems Society
- Henry Schein, Inc.
- International Cemetery and Funeral Association
- Johns Hopkins University
- Joint Commission on Accreditation of Healthcare Organizations
- Kaiser Permanente
- LabCorp
- National Funeral Directors Association
- Pharmaceutical Research and Manufacturers of America
- University of Pittsburgh Medical Center

INFORMATION TECHNOLOGY SECTOR

PARTNERSHIP

Critical Information Technology (IT) Sector functions support the sector's ability to produce and provide high assurance IT products and services for all critical infrastructure and key resources (CIKR) sectors, citizens, businesses, and employees. Collaboration among public and private sector security partners is critical to ensure the protection and resilience of the IT Sector functions upon 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 Office of Cybersecurity and Communications, within the Department of Homeland Security (DHS), serves as the IT Sector-Specific Agency. The Cross-Sector Cyber Security Working Group facilitates coordination on cross-sector cybersecurity issues.

VISION

The IT Sector provides an infrastructure upon which all other CIKR sectors rely. As such, the IT Sector's vision is to ensure an infrastructure that is secured, assured, and resilient and that any disruptions or manipulations of IT Sector critical functions are brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States. Such a vision supports the following:

- 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 deliver minimum essential public services.
- The orderly functioning of the economy.

GOALS

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

- Identify, assess, and manage risks to the IT Sector's critical functions and their 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 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 resiliency and protective posture of the IT Sector. Some of the sector's accomplishments over the past year include the following:

- Conducted the baseline IT Sector Risk Assessment, bringing together over 70 subject matter experts from government and the private sector to evaluate threats, vulnerabilities, and consequences to the Nation's IT infrastructure.
- Responded to daily cyber attacks and organized robust, sector-wide responses to major cyber threats.
- Developed a research and development (R&D) information-sharing framework to enable the private sector and government to conduct complementary IT CIKR R&D activities without compromising competitive advantages.

KEY INITIATIVES

Key initiatives within the IT Sector include the following:

- Promoting response and recovery by coordinating with DHS and other sectors on cyber incidents.
- Building on the sector baseline risk assessment to assess and manage cross-sector risks and interdependencies and to refine metrics and protective programs.

GCC Members

- National Association of State Chief Information Officers
- U.S. Department of Commerce
- U.S. Department of Defense
- U.S. Department of Homeland Security
- U.S. Department of Justice
- U.S. Department of State
- U.S. Department of the Treasury

SCC Members

- AC Technology, Inc.
- Afilias USA, Inc.
- Anakam, Inc.
- Arxan Defense Systems, Inc. & Dunrath Capital
- Bearing Point
- Bell Security Solutions Inc.
- Business Software Alliance
- Center for Internet Security
- Cisco Systems, Inc.
- Computer and Communications Industry Association
- Computer Associates International
- Computer Sciences Corporation
- Computing Technology Industry Association
- Concert Technologies
- Core Security Technologies
- Cyber Pack Ventures, Inc.
- Cyber Security Industry Alliance
- Deloitte & Touche LLP
- Detica
- eBay
- EDS
- Electronic Industries Alliance
- EMC Corporation
- Entrust, Inc.
- EWA Information & Infrastructure Technologies, Inc.
- General Atomics
- General Dynamics
- Green Hills Software
- Google
- Hatha Systems
- IBM Corporation
- IBM Internet Security Systems, Inc.
- Information Systems Security Association

- Coordinating across CIKR sectors on response and recovery activities through the IT Information Sharing and Analysis Center (ISAC) and United States Computer Emergency Readiness Team (US-CERT).
- Enhancing information sharing and increasing situational awareness through IT information sharing and analysis and cybersecurity outreach and awareness.
- Developing an R&D information exchange framework.
- Providing leadership for cross-sector cybersecurity through the Cross Sector Cyber Security Working Group and other policy information sharing and protective security programs, including the US-CERT.

PATH FORWARD

Numerous steps will be taken to address the challenges in the sector. These steps include the following:

- Migrate from a sector-wide risk assessment posture to a sector-wide risk management posture.
- Aid exercise planners in other CIKR sectors with integrating cybersecurity elements affecting public and private sector exercise participants into exercise goals, objectives, scenarios, and execution.
- Continue to work across various sectors to help sector leaders understand and manage interdependency risks.
- Continue to engage international entities in exercises and operational activities to expedite awareness, planning, response to, and recovery from incidents.
- Set mutually agreed-upon requirements for participating representatives and for interaction and information sharing with the IT SCC, the IT GCC, and the IT-ISAC.
- Plan and implement the National Cyber Exercise: Cyber Storm III.
- Build a joint industry-government Cyber Operations Center.
- Develop a Concept of Operations to ensure continued coordination and cohesion between industry and government in prioritizing and mitigating the risks identified in the baseline IT Sector Risk Assessment (ITSRA).
- Develop version 2.0 of the ITSRA.

"[T]he IT Sector has made considerable progress in its CIKR protection and resilience agenda. Sector partners completed a credible and defensible baseline IT Sector Risk Assessment (ITSRA)."

2009 Information Technology Sector Annual Report

"The broad spectrum of public and private sector entities that provide the critical functions and subfunctions compel the sector to rely upon partnerships across private industries, DHS, Federal agencies, and State, local, tribal, and territorial governments."

2009 Information Technology Sector Annual Report

Critical IT Sector Functions

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

- Intel Corporation
- Information Technology Information Sharing and Analysis Center
- International Systems Security Engineering Association
- Internet Security Alliance
- International Security Trust and Privacy Alliance
- ITT Corporation
- Juniper Networks
- KPMG LLP
- L-3 Communications
- Lancope, Inc
- LGS Innovations
- Litmus Logic
- Lockheed Martin
- Lumeta Corporation
- McAfee, Inc.
- Microsoft Corporation
- Neustar
- Northrop Grumman
- NTT America
- One Consulting Group
- One Enterprise Consulting Group, LLC
- PerotSystems
- R & H Security Consulting LLC
- Raytheon
- Reclamere
- Renesys Corporation
- Seagate Technology
- Sentar Inc
- Siemens Healthcare
- SI International
- Sun Microsystems, Inc
- Symantec Corporation
- System 1
- TechAmerica
- Telecontinuity, Inc.
- Terremark World Wide
- TestPros, Inc.
- Triumfant
- Unisys Corporation
- U.S. Internet Service Provider Association
- VeriSign
- Verizon
- 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 Sector Coordinating Council (SCC) of the sectors. The U.S. 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.

VISION

The NMI Sector is committed to ensuring that the symbols of our Nation remain protected and intact for future generations. In the course of protecting our landmarks, the sector will ensure 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 among 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:

- Continue to review sector criteria to ensure a clear definition of NMI assets.
- Delineate and define roles and responsibilities for sector security partners.
- Continue to 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 Government Coordinating Council (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 available resources and robust security, technology, and practices contingent on agency mission priorities while preserving the appearance and accessibility of NMI Sector assets.
- 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 have continued to preserve and enhance the protective posture and resiliency of the NMI Sector. Some of the sector's accomplishments over the past year include the following:

- Conducted a comprehensive study of the psychosocial impacts of a terrorist attack on an NMI asset, through the Homeland Security Institute in support of U.S. Department of Homeland Security Office of Science and Technology.
- Consolidated oversight responsibilities for NMI assets on the National Mall, as well as at the Statue of Liberty, under one senior security manager.
- Commissioned a comprehensive risk assessment to determine the likely chemical, biological, and radiological threats that may be used directly against Smithsonian facilities on the National Mall or nearby high-profile facilities.
- Opened a new operations center capable of providing situational awareness and decisionmaking support to the DOI's senior leaders during all-hazard emergencies on a 24-hour basis.

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 and resilient sector.

Key initiatives within the sector include:

- Completing blast assessments at all NMI assets.

GCC Members

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

- Implementing civil aviation restrictions around critical infrastructure and key resources (CIKR) assets located outside the Washington, D.C. metropolitan area.
- Participating in Buffer Zone Protection Plan development and other security-related initiatives, such as the Lower Manhattan Protection Zone initiative.
- Promoting the use of the Homeland Security Information Network (HSIN) secure portal by GCC partners.

PATH FORWARD

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

- Assess the relative value of strategies for mitigating the psychosocial impacts of terrorism.
- Develop a methodology to provide dollar estimates of the costs related to the psychosocial impacts of terrorism over the longer term (months and years after an attack).
- Conduct additional research into the nature, extent, and duration of cognitive impacts from terrorist attacks, such as the "rally effect."
- Conduct a broader survey and convene a series of focus groups to support the development of metrics that will allow the NMI Sector to rank various national monuments and icons by the symbolic value the American people attribute to them.
- Continue to promote and facilitate intelligence and information sharing, effective security practices, CIKR Science and Technology Directorate initiatives, and training opportunities among the GCC partners.

"The NMI Sector GCC provides an effective mechanism for coordinating CIKR protective strategies and activities, policy, and communication across and between Federal Government agencies and throughout the NMI Sector to support the Nation's homeland security mission."

2009 National Monuments and Icons Sector Annual Report

"The NMI Sector has partnered with the Government Facilities Sector to coordinate outreach to State, local, tribal, and private entities."

2009 National Monuments and Icons Sector Annual Report

"The NMI Sector developed its own HSIN portal to enable sector partners to share information quickly concerning all-hazard threats and potential protective measures that have been used successfully."

2009 National Monuments and Icons Sector Annual Report

- U.S. 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 the United States' 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 Nuclear Government Coordinating Council (NGCC) administer special working groups, as well as three subcouncils addressing issues specific to research and test reactors, radioisotopes, and cybersecurity. The U.S. Department of Homeland Security (DHS) Office of Infrastructure Protection serves as the Sector-Specific Agency (SSA) for the Nuclear Sector.

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 critical infrastructure and key resources (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, security, and resiliency of the Nuclear Sector. The sector's accomplishments over the past year include the following:

- Completed an Integrated Pilot Comprehensive Exercise at the Limerick Nuclear Generating Station in December 2008.
- Implemented a voluntary program to improve the security of Research Test Reactor facilities.
- Implemented 466 voluntary security enhancements identified during Comprehensive Reviews conducted between 2005 and 2007.
- Finalized new rule updating security requirements for the Nation's civilian nuclear power reactors.
- Implemented a national program to harden radiological facilities and install in-device delay kits to make unauthorized removal of radioactive materials from high-risk irradiators more difficult.
- Launched the National Source Tracking System to securely inventory high-risk radiation sources licensed in the United States.
- Published a new rule requiring nuclear power plants to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks.

KEY INITIATIVES

The Nuclear Sector and its security partners are 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:

- Implementing additional voluntary security enhancements identified during Comprehensive Reviews.

GCC Members

- Nuclear Regulatory Commission
- State of Florida, Department of Health
- State of Massachusetts, Department of Public Health
- State of Pennsylvania, Department of Environmental Protection
- State of Texas, Department of Regulatory Services
- U.S. Department of Defense
- U.S. Department of Energy
- U.S. Department of Homeland Security
- U.S. Department of Justice
- U.S. Department of State
- U.S. Department of Transportation
- U.S. Environmental Protection Agency

- Conducting emergency preparedness drills using hostile action-based scenarios as initiating events.
- Facilitating response to security threats at facilities with nuclear or radiological materials through the Responder Training Program.
- Amending security regulations and adding security requirements pertaining to nuclear power reactors.
- Conducting force-on-force inspections to assess a nuclear plant's physical protection measures to defend against the "design basis threat."
- Assessing the security and safeguards performance of power plant licensees subject to the requirements of Code of Federal Regulations (CFR) Title 10 Part 73 or Nuclear Regulatory Commission (NRC) orders.

PATH FORWARD

The Nuclear Sector still faces some CIKR protection and resilience challenges, including increasing the resiliency of the radioisotopes supply chain, developing a normalized risk assessment framework for a heterogeneous set of assets and systems, developing an integrated response capability, and ensuring the security of cyber-based systems. The sector will take the following steps to address these challenges:

- Participate in the Critical Foreign Dependencies Initiative and continue to collaborate with the Departments of Energy and State and other partners to address radioisotope supply and disposition challenges.
- Incorporate into subsequent assessments the lessons learned from the sector's 2009 Strategic Homeland Infrastructure Risk Analysis program.
- Continue to coordinate with State and local authorities and with the private sector, as appropriate, to promote adequate, consistent, and integrated response preparations across the sector.
- Continue to identify cybersecurity risks that could potentially affect the Nuclear Sector and determine mitigation strategies through engagement with the National Cyber Security Division's (NCSD) Cross-Sector Cyber Security Working Group and Industrial Control Systems Joint Working Group.

"[T]he NRC has published a new rule that will require power plant licensees to submit a cybersecurity plan for NRC review and approval by November 23, 2009."

2009 Nuclear Sector Annual Report

"An influential October 2008 assessment of the CIKR-protection partnership by the National Infrastructure Advisory Council cited CROWN as one of the 'tangible accomplishments of the sector partnership."

2009 Nuclear Sector Annual Report

"[The Integrated Pilot Comprehensive Exercise] was unique in bringing together a diverse range of security partner tactical response teams to work through multiteam tactical integration in the context of a response to a security event at a nuclear power generation facility."

2009 Nuclear Sector Annual Report

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 (P&S) 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 & Shipping Sector is mainly composed of 4 large, integrated carriers that represent 93% 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).

VISION

Ensure continuity of operations, ease of use, and public confidence in the Postal and Shipping Sector by creating a multilayered 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 incident-reporting mechanisms and awareness and outreach programs with the law enforcement and intelligence communities to facilitate a better understanding of the information requirements of the Postal and Shipping Sector.
- Ensure timely, relevant, and accurate threat reporting from the law enforcement and intelligence communities to key decisionmakers 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 Systems, Energy, Information Technology, Communications, Commercial Facilities, and Healthcare and Public Health Sectors.
- Facilities: Implement risk-based security measures for transportation assets, processing and distribution centers, and IT centers that are tailored to the size of implementing organizations and scalable to accommodate both routine protective requirements and periods of heightened alert.
- Personnel: Work to deny terrorists the ability to exploit or replicate the trusted access that P&S Sector personnel have to public and private facilities for collecting, transporting, and delivering parcels and letters.
- Parcels and Letters: Work to rapidly detect, prevent further movement of, and neutralize chemical, biological, or radiological material inserted into the P&S system for delivery to intended targets.
- Create public-private forums to identify roles and responsibilities for responding to a terrorist attack, threats and disruptions, crippling attacks (cyber or physical), or other intentional or unintentional incidents and develop continuity of operations plans to ensure that the sector can continue to move parcels and letters to intended recipients.
- Identify critical commodities that must be delivered to enable an effective response to a national or regional critical emergency and develop coordinated plans to ensure that critical commodities are delivered in a timely and effective manner.
- 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 national, regional, and local public communication protocols to inform U.S. citizens 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. The sector's accomplishments over the past year include the following:

- Developed the Postal and Shipping Sector business plan.
- Created and approved the Critical Infrastructure and Key Resources (CIKR) asset list.
- Completed asset site reviews.
- Identified CIKR Tier 1 and Tier 2 lists.
- Identified sector risk mitigation activities.
- Tracked the output measures of risk mitigation activities.
- Prepared the 2009 Sector Annual Report.
- Prepared the 2009 Sector Specific Plan Annual Review.

KEY INITIATIVES

The Postal and Shipping Sector is implementing various programs to enhance the security and resiliency of its assets.

GCC Members

- U.S. Department of Defense
- U.S. Department of Health and Human Services
- U.S. Department of Homeland Security
- U.S. Department of Justice

Key initiatives within the sector include:

- Enhancing frontline employee awareness.
- Enhancing cybersecurity awareness.
- Strengthening supply chain security awareness.
- Identifying integrated carrier vulnerabilities.
- Identifying supply chain vulnerabilities.
- Participating in P&S Sector security exercises.
- Identifying cross-sector risks.
- Supporting and participating in the P&S Sector Cities Readiness Initiative.
- Improving sector resiliency.
- Enhancing emergency preparedness.
- Facilitating the sharing of security information.

PATH FORWARD

The Postal and Shipping Sector faces challenges in securing numerous and easily accessible assets, large and diverse information systems, and a wide array of transportation systems. Numerous steps will be taken as the Postal and Shipping Sector moves forward in securing its resources, including the following:

- Engage the threat analytical community to provide regular threat analysis for the sector.
- Identify a methodology for developing threat, vulnerability, and consequence assessments.
- Engage the sector to assess sector dependencies and interdependencies.
- Communicate cybersecurity improvement programs to the sector.
- Develop a voluntary security resilience evaluation for sector components that aims to identify preparedness standards that are specific to the sector.
- Engage P&S trade associations and other entities that reach the components of the P&S supply chain to participate in the development and active implementation of a voluntary security resilience program.
- Identify and define sector training and communication requirements that will allow sector components to improve the preparedness, resiliency, and security of their operations.
- Continue to ensure that timely threat information is shared across the P&S Sector and that the information is effectively disseminated.
- Engage the P&S Sector to test resiliency and recovery in the event of an incident to ensure that the roles in responding to an incident are clear and will be effective.
- Understand the full scope of cybersecurity issues and vulnerabilities, develop mitigation strategies, and communicate cybersecurity improvement programs to the sector.

"Americans depend on the P&S Sector for the reliable delivery of more than 200 billion letters and packages annually."

2009 Postal and Shipping Sector Annual Report

"P&S GCC and SCC partners participated in emergency responses with TSA as a result of four hurricanes that hit the Gulf Coast from mid-September to early October 2008."

2009 Postal and Shipping Sector Annual Report

"In FY 2008, postal inspectors responded to 2,894 incidents nationwide involving unidentified suspicious powders and liquids reported by postal employees, customers, or other Federal agencies."

2009 Postal and Shipping Sector Annual Report

"To strengthen CIKR protection, resiliency, and other security measures, P&S Sector owners and operators, including postal inspectors and National Preparedness Group staff, conducted more than 1,000 security assessment reviews at postal facilities nationwide."

2009 Postal and Shipping Sector Annual Report

SCC Members

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

TRANSPORTATION SYSTEMS SECTOR

PARTNERSHIP

The Transportation Sector is a vast, open network of interdependent systems that moves millions of passengers and billions of tons of goods annually. The Transportation Sector partnership framework includes a Government Coordinating Council (GCC), a Sector Coordinating Council (SCC) expected to form by 2010, and subsector GCCs and SCCs for each of the six transportation modes: Aviation, Maritime, Mass Transit, Highway, Freight Rail, and Pipeline. The SCCs include leading associations, owners and operators, and other private sector entities with transportation security responsibilities; and the GCCs consist of members from key Federal, State, and local agencies. The Transportation Security Administration serves as the Sector-Specific Agency (SSA) for the Transportation Sector, and the U.S. Coast Guard serves as the Maritime Mode SSA.

VISION

The Transportation Sector's vision is 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 and 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 systems security.

SELECTED ACCOMPLISHMENTS

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

- Achieved first milestone for screening of cargo on passenger aircraft.
- Aligned transportation grant projects to reduce security risks in most vulnerable regions.
- Expanded sector security exercise program across all modes.
- Conducted 62 Area Maritime Security Plan (AMSP) exercises.
- Developed key risk reduction programs such as Visible Intermodal Protection and Response (VIPR) and Transportation Worker Identification Credential (TWIC).

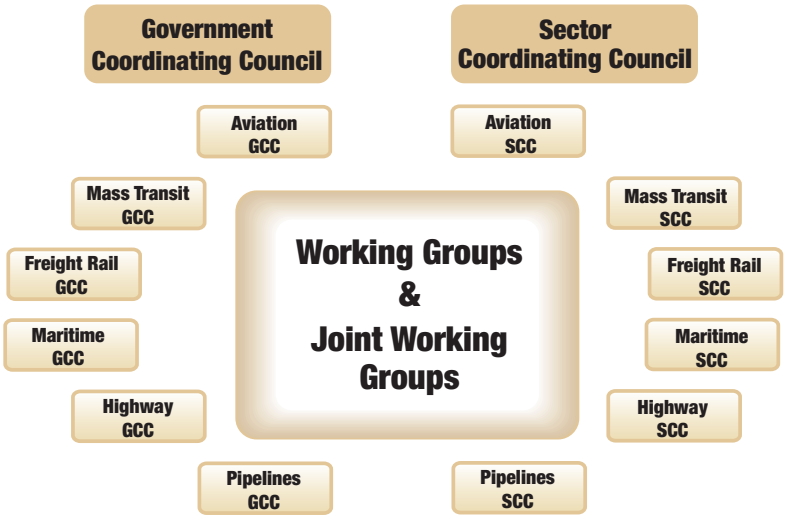
KEY INITIATIVES

The Transportation Sector is undertaking a wide variety of initiatives to continue improving the security and safety of sector assets. Several of these initiatives involve the modal GCCs bringing together numerous government agencies to collaborate on security efforts, which range 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:

- Screening and vetting of workers, travelers, and shippers through the TWIC and Secure Flight programs.
- Securing critical physical infrastructure through the National Tunnel Security Initiative, General Aviation Airport Security Measurements, and AMSPs.
- Implementing risk-mitigation operational practices through the Toxic Inhalation Hazard Risk Reduction Program and the Container Security Initiative.

Transportation Sector Partnership Framework



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

- Implementing unpredictable operational deterrents through the Federal Air Marshal Service Mission Deployments and VIPR Program.
- Conducting security awareness and response training through the Evolution and Certified Cargo Screening Programs.
- Conducting security awareness and response training programs such as Federal Flight Deck Officers, Flight Crewmember Self-Defense Training, and Mass Security Training.
- Conducting multimodal drills and exercises with emphasis on preparedness and response through the Intermodal Security Training and Exercise Program (I-Step).
- Keeping the public and other security partners aware of the sector's security efforts through the Security Training, Operational Readiness, and Maritime Community Awareness Program.
- Leveraging technological advances to improve security efforts through the Advanced Technology X-ray for Personal Property Screening and Electronic Boarding Pass programs.
- Raising the security baseline and increasing the amount and quality of security plan development through the Rail Transportation Security Final Rule program.
- Evaluating the vulnerability of critical transportation infrastructure through the Baseline Assessment for Security Enhancement and Airport Vulnerability Assessment programs.
- Developing a comprehensive strategic approach for securing cybersecurity infrastructure.

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:

- Complete and apply the revised risk management framework.
- Encourage the sharing of risk assessments and products by sector participants.
- Improve consequence models for evaluating the sector's critical infrastructure and key resources.
- Improve the sector's awareness of interdependencies with other sectors and other agencies to identify and address cross-sector security gaps.
- Identify critical cybersecurity systems and vulnerabilities, and increase the use of technology before, during, and after incidents, including the Homeland Security Information Network (HSIN) and mapping and tracking technologies, such as geographic information systems and global positioning systems.

"The recently implemented International Ship and Port Facility Security (ISPS) is one of the most meaningful mechanisms for partner engagement in the security program evaluation."

2009 Transportation Sector Annual Report

"The Quadrilateral Working Group (the Quad) provides opportunities for the European Union, the United States, Australia, and Canada to discuss priority transportation security issues and develop high-level responses to shape national and international security policy."

2009 Transportation Sector Annual Report

"The National Explosives Detection Canine Team Program continued to augment local explosives detection capabilities by providing partial funding, training, certification, and management assistance."

2009 Transportation Sector Annual Report

"The sector is committed to improving threat awareness through increased training and outreach and targeted communications with both transportation service providers and users."

2009 Transportation Sector Annual Report

This section may not represent a consensus report by all the modes within the Transportation Sector.

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 sewage 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 owners 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 U.S. Environmental Protection Agency (EPA) serves as the Sector-Specific Agency (SSA) for the Water Sector.

VISION

The Water Sector's 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

Water Sector partners are collaborating to achieve the following 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 following:

- Established Regional Laboratory Response Plans and conducted functional exercises of those plans. To date, 11 functional exercises have been conducted in all 10 EPA regions involving 44 State, 6 Federal, 12 water utility, and 2 city laboratories.
- Increased investments and efforts in promoting the establishment of intrastate mutual aid and assistance agreements, such as Water-Wastewater Agency Response Networks (WARNs). To date, 42 states and the National Capital Region have established WARNs.
- Worked with the United States Army Corps of Engineers to incorporate Emergency Support Function 3 (ESF-3) protocols into the ESF-3 Field Guide as a Water Infrastructure Annex.
- Completed first annual performance metrics process for the Water Sector covering measures for utility and "other actor" agencies, including States, Federal agencies, and Water Sector associations; conducting second annual performance metrics process.
- Conducted numerous Site Assistance Visits, worked with communities in the Buffer Zone Protection Program, and conducted Enhanced Critical Infrastructure Protection visits to high-consequence water utilities to assist in vulnerability reduction.
- Prepared the *Roadmap to Secure Control Systems in the Water Sector*, which is a unified security strategy containing specific goals, milestones, and activities to mitigate cybersecurity risk over the next 10 years.
- Completed a comprehensive inventory of Water Sector research and development (R&D) projects, identified capability gaps, and prioritized those gaps using an analytical process.

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. These 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:

- Implementing the Water security initiative

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 and City Health Officials
- National Association of Regulatory Utility Commissioners
- U.S. Department of Agriculture
- U.S. Department of Defense
- U.S. Department of Health and Human Services
- U.S. Department of Homeland Security
- U.S. Department of State
- U.S. Department of the Interior
- U.S. Environmental Protection Agency

that aims to detect and appropriately respond to drinking water contamination threats and incidents.

- Enhancing the security of drinking water utilities through development of a laboratory network known as the Water Laboratory Alliance.
- Developing an all-hazards consequence management planning document; evaluating preparedness, emergency response, and recovery priorities; and identifying actions needed to implement priorities, through use of a Critical Infrastructure Partnership Advisory Council (CIPAC) working group.
- Evaluating progress made toward critical infrastructure protection.
- Conducting and updating risk assessments.
- Preparing and revising emergency response plans.
- Developing a generalized consequence analysis tool, Water Health and Economic Analysis Tool, to quantify human health and economic consequences for a variety of asset-threat combinations that pose a risk.
- Conducting numerous Site Assistance Visits through protective security advisors.

PATH FORWARD

The Water Sector is implementing various programs to enhance the security and resiliency of its assets.

Key initiatives within the sector include the following:

- Follow up on sector–specific metrics.
- Continue sector strategic planning, cybersecurity, and decontamination.
- Coordinate R&D efforts.
- Advance WARN use and business continuity planning.
- Continue to identify and address interdependencies.
- Enhance ongoing partnership efforts of the Water SCC, GCC, and CIPAC working groups.

"The Roadmap to Secure Control Systems in the Water Sector is a unified security strategy to mitigate the risks associated with cyber systems."

2009 Water Sector Annual Report

"The CIPAC Water Sector Decontamination Working Group finalized a report, *Recommendations and Proposed Strategic Plan – Water Sector Decontamination Priorities*. The proposed strategy identified and prioritized decontamination and recovery issues and needs for returning both drinking water and wastewater systems to service after a contamination event."

2009 Water Sector Annual Report

"In early 2009, EPA coordinated with the Association of State Drinking Water Administrators (ASDWA) on identifying anecdotal information about State efforts related to water security. Many States conducted security related initiatives or projects that either specifically or as a whole improved the security position of the Water Sector."

2009 Water Sector Annual Report

SCC Members

- American Water
- American Water Works Association (AWWA)
- AWWA Research Foundation
- Association of Metropolitan Water Agencies
- Bean Blossom Patricksburg Water Corporation
- Beaufort-Jasper Water & Sewer Authority
- Boston Water and Sewer Commission
- Breezy Hill Water and Sewer Company
- City of Portland Bureau of Environmental Services
- District of Columbia Water and Sewer Authority
- Fairfax Water
- Greenville Water System
- King County Department of Natural Resources and Parks
- Lafeyette Utilities System
- National Association of Clean Water Agencies
- National Association of Water Companies
- National Rural Water Association
- New York City Department of Environmental Protection
- Pima County Wastewater Management Department
- Tempe Water Utilities
- Trinity River Authority of Texas
- United Water
- Water Environment Federation
- Water Environment Research Foundation

Homeland
Security