2010

Critical Infrastructure Partnership Advisory Council *Annual*

Homeland Security

2010 CRITICAL INFRASTRUCTURE PARTNERSHIP ADVISORY COUNCIL ANNUAL

CONTENTS

OVERVIEW

Introduction

Protecting and ensuring the resilience of the Nation's critical infrastructure requires 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 public and private sector partners, leads the national effort to mitigate risk to the Nation's critical infrastructure through the development and implementation of an effective national infrastructure protection program. The sector partnership model serves as the primary organizational structure for coordinating critical infrastructure efforts and activities. The Critical Infrastructure Partnership Advisory Council (CIPAC) directly supports the sector partnership model by providing a legal framework for members of the Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs) to engage in joint critical infrastructure protection and resilience efforts and serves as a forum for government and private sector partners to participate in a spectrum of activities, including:

- Planning, developing, and implementing critical infrastructure protection and resilience programs
- Coordinating operational activities related to critical infrastructure protection and resilience, including incident response and recovery
- Developing and supporting national policies and plans, including the National Infrastructure Protection Plan (NIPP) and Sector-Specific Plans (SSPs)

CIPAC members include private sector critical infrastructure owners and operators or their representative trade or equivalent associations from the respective SCC, as well as representatives of Federal, State, local, and tribal entities (including their representative trade or equivalent associations) that make up the corresponding GCC. 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. Renewal of CIPAC Establishment was subsequently announced through Federal Register Notices published on April 30, 2008 and April 22, 2010.

The 2010 CIPAC Annual summarizes the infrastructure protection and resilience activities and accomplishments of the 18 critical infrastructure sectors and four cross-sector councils of the NIPP partnership.

NIPP Partnership

An SCC is the principal entity for owners and operators to coordinate with the government on critical infrastructure protection and resilience activities and issues. A GCC is the government counterpart for each SCC and facilitates interagency and cross-jurisdictional coordination. The 18 critical infrastructure sectors have established 16 SCCs and 18 GCCs.

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

- The CIKR Cross-Sector Council—addresses cross-sector issues and interdependencies among the SCCs. The Council is comprised of the leadership of each of the SCCs
- The 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 the Sector-Specific Agencies and other Federal agencies that are relevant to critical infrastructure protection and resilience
  - The SLTTGCC consists of homeland security directors or their equivalents or representatives from State, local, tribal, and territorial governments
- The 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 or geographic area

Key Initiatives

Public and private sector partners are currently implementing a wide range of activities to improve the protection and resilience of the Nation's critical infrastructure. 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

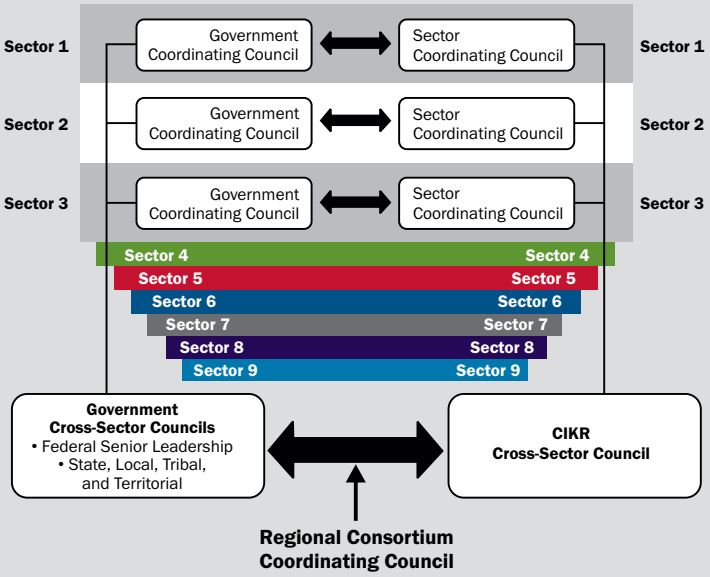
- Raising security awareness through guidance programs, documents, and plans
- Conducting or updating risk assessments
- Maintaining emergency preparedness and business continuity plans
- Participating in exercises to enhance emergency preparedness
- Improving emergency management communication
- Developing and distributing materials on critical infrastructure protection and resilience best practices and lessons learned
- Developing and participating in critical infrastructure protection training Webinars
- Establishing cross-sector committees and working groups under the CIKR Cross-Sector Council
- Coordinating with the 18 sectors through the SLTTGCC to develop a program of sector liaisons to provide regional expertise on infrastructure protection and resilience

Path Forward

Looking forward, critical infrastructure partners will continue to increase participation in sector partnership activities and incorporate more infrastructure owners and operators across the Nation into communication, information sharing, and training on critical infrastructure protection and resilience activities. Key elements include the following:

- Expand participation in the CIKR Information Sharing Environment and improving its effectiveness and efficiency through mission-driven requirements, including HSIN-CS
- Improve awareness of interdependencies among sectors and agencies to help identify and address cross-sector infrastructure protection gaps
- Leverage existing channels of communication and building additional channels through State and local partnerships with infrastructure owners and operators in communities
- Expand the use of metrics to measure effectiveness and encourage progress toward critical infrastructure protection and resilience goals
- Disseminate products developed by the critical infrastructure partnership to an increasing number of infrastructure owners and operators across the Nation
- Support private sector research and development efforts

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."

Source: 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."

Source: 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 the wide array of CIKR partners."

Source: 2009 National Infrastructure Protection Plan

CIKR CROSS-SECTOR COUNCIL

Partnership

The CIKR Cross-Sector Council (the Council) addresses cross-sector issues and interdependencies among the Sector Coordinating Councils (SCCs) and comprises the leadership of each of the SCCs. The Partnership for Critical Infrastructure Security (PCIS) provides this representation with support from the Department of Homeland Security (DHS) Executive Secretariat. The primary activities of the Council include providing senior-level, cross-sector strategic coordination through partnership with DHS and the Sector Specific Agencies; supporting and participating in the development and implementation of the NIPP and the Sector-Specific Plans; and identifying and disseminating best practices for critical infrastructure protection and resilience across the sectors.

Vision

The Council facilitates close cross-sector collaboration between the private sector and the Government to improve the security and resilience of critical infrastructure assets, functions, and sectors.

Goals

The Council pursues four key goals to advance its mission to increase collaboration among SCCs and the Government. These four goals include the following:

- ***Partnership leadership***—provide proactive leadership on leveraging the partnership model to facilitate private cross-sector collaboration with the Government
- ***Cross-Sector leadership***—provide leadership on identifying cross-sector and interdependency risks and providing solutions to manage those risks
- ***Sector assistance***—provide leadership on strengthening SCCs
- ***Effectiveness***—improve outreach among sectors and with the Government

Selected Accomplishments

The Council's recent accomplishments include the following:

- Initiated a comprehensive cross-sector study on critical interdependencies in partnership with the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) and the Regional Consortium Coordinating Council (RCCC) to inform regional and local decisionmakers about the potential for specific, cascading effects across multiple sectors during an event in their area, as well as the far reaching implications for all critical infrastructure partners
- Participated in CIKR Roundtable discussions with Secretary Napolitano to highlight successes, concerns, and opportunities for the Council and DHS
- Continued active and leadership participation as two of the three co-chairs to the Cross-Sector Cyber Security Working Group, a collaborative public-private forum to address cybersecurity issues affecting multiple sectors
- Elevated the Council's participation in the design and development of objectives, scenarios, and the execution of National Level Exercises (NLE), and also provided the Chair of the National Private Sector Working Group for NLE-10 and NLE-11
- Facilitated emerging threat briefings between DHS and specific sectors
- Increased awareness of the Council's activities and cross-sector issues through meetings with Congressional leaders and DHS senior executives
- Assisted in follow-up efforts for the 60-Day Cyberspace Policy Review, Cyber Incident Response Plan, and contributed to the National Strategy for Trusted Identities in Cyberspace
- Co-chairs the Information Sharing Policy and Strategy Working Group
- Integrated additional stakeholders into regular PCIS meetings and activities, such as senior representatives of the SLTTGCC, the RCCC, and the National Council of Information Sharing and Analysis Centers, which improved coordination between participating organizations and expedited resilience planning, information sharing, and crisis management at all levels

Key Initiatives

The Council organizes its efforts on initiatives via committees made up of member representatives. There are currently several committees underway, including the following:

- ***Cross-Sector Cyber Security Working Group***—focuses on developing collaborative approaches for improving the Nation's cybersecurity and is co-chaired by the Council and DHS, under CIPAC
- ***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 critical infrastructure community; educates key stakeholders on the Council's activities and the larger critical infrastructure security effort; and maintains Council awareness of government activities related to critical infrastructure matters

CIKR CROSS-SECTOR COUNCIL MEMBERS

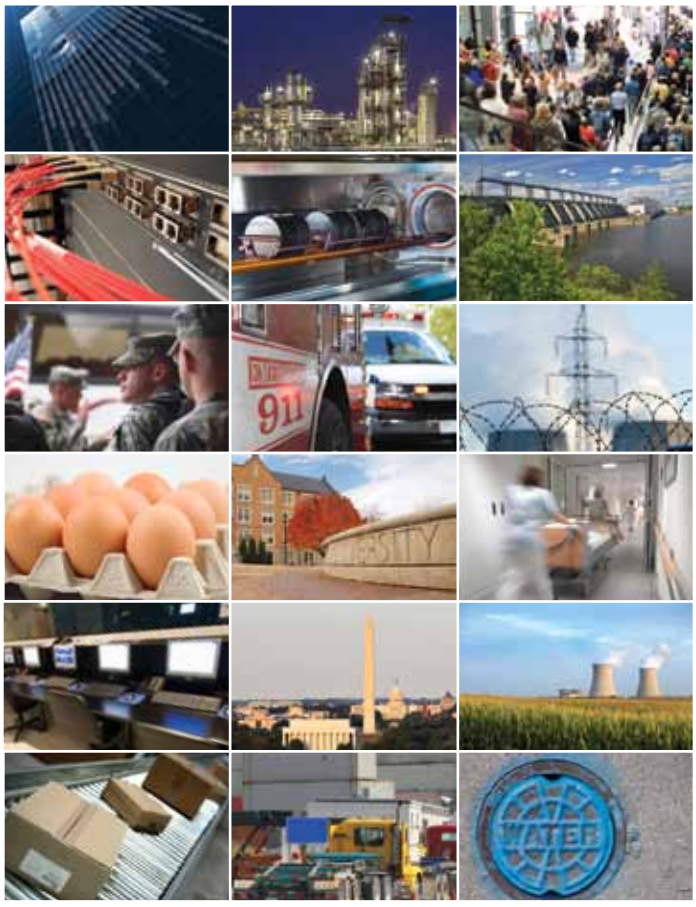
- Banking and Finance
- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy—Electricity
- Energy—Oil and Natural Gas
- Food and Agriculture
- Healthcare and Public Health
- Information Technology
- Nuclear
- Postal and Shipping
- Transportation—Aviation Mode
- Transportation—Highway and Motor Carrier Mode
- Transportation—Maritime Mode
- Transportation—Mass Transit Mode
- Transportation—Pipeline Mode
- Transportation—Freight and Rail Mode
- Water

- ***Exercise Committee***—provides input from the private sector critical infrastructure community on the exercise design and implementation process within DHS and the larger exercise community
- ***Interdependencies Committee***—works to identify and better understand interdependencies within the critical infrastructure community and foster better
- ***Regional, State, and Local Information-Sharing Committee***—helps create security and all-hazard information-sharing networks at the regional, State, and local levels and assists with the coordination of information sharing between regional, State, and national entities sharing between regional, State, and national entities

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



Critical Infrastructures

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

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 critical infrastructure sector, as well as several additional agencies named in HSPD-7.

Key Activities

The FSLC's primary activities include the following:

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

Selected Accomplishments

Recent accomplishments of FSLC agencies include the following:

- Continued to implement individual SSPs, emphasizing resilience and cybersecurity as applicable to each sector
- Expanded engagement with State, local, tribal, territorial, and regional critical infrastructure partners through the State, Local, Tribal, and Territorial Government Coordinating Council; the Regional Consortium Coordinating Council; and individual sector efforts
- Worked with partners in government and the private sector to complete a triennial review and revision of the SSPs and finalize for publication
- Participated in the review and supported revisions to HSPD-7 to reflect the evolution of NIPP programs and maturation of the sector partnership
- Expanded the use of Homeland Security Information Network-Critical Sectors by launching and enhancing sector portals to share relevant and timely information with critical infrastructure partners
- Developed the *2010 Sector CIKR Protection Annual Reports* (summaries follow) and enhanced measurement of critical infrastructure protection and resilience progress
- Collaborated on cyber initiatives through the Cross-Sector Cyber Security Working Group

FEDERAL SENIOR LEADERSHIP COUNCIL MEMBERS

- National Security Staff
- Nuclear Regulatory Commission
- Office of the Director of National Intelligence
- Office of Management and Budget
- U.S. Army Corps of Engineers
- U.S. Department of Commerce
- U.S. Department of Education
- U.S. Department of Homeland Security
  - Office of Infrastructure Protection
  - Science and Technology Directorate
  - Sector Specific Agency Executive Management Office
- U.S. Department of Justice
  - Federal Bureau of Investigation
- U.S. Department of State
- U.S. Department of Transportation

Membership

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

Sector-Specific Agency	Critical Infrastructure and 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	Communications Information Technology
Federal Protective Service	Government Facilities
Transportation Security Administration	Postal and Shipping
Transportation Security Administration, United States Coast Guard	Transportation Systems

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

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

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

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

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

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

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

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

Source: 2009 National Infrastructure Protection Plan

STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENT COORDINATING COUNCIL

Partnership

The State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) 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 integrating State, local, tribal, and territorial (SLTT) governments into the critical infrastructure 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 critical infrastructure protection. The SLTTGCC conducts most of its activities through six working groups: Automated Critical Asset Management System (ACAMS), Chemical Facility Anti-Terrorism Standards (CFATS), Communication and Coordination Working Group, Information Sharing and Collaboration Working Group, Policy and Planning Working Group, and Regional Partnership Working Group.

Vision

The SLTTGCC strives to integrate SLTT governments into critical infrastructure national strategies to assure a safe, secure, and resilient infrastructure.

Goals

SLTT 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 that State, local, tribal, and territorial homeland security officials or their designated representatives are integrated as active participants in national critical infrastructure 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 critical infrastructure SLTT government partners into the critical infrastructure information-sharing environment
- Engage with and 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:

- Continued dialogue with the Infrastructure Security Compliance Division on chemical security, in particular the implementation of the CFATS
- Assisted in the design and implementation of the CFATS
- Recommended the expansion and improvements to the Automated Critical Asset Management System (ACAMS)
- Developed guidelines for identifying regional critical infrastructure protection partners
- Contributed to the Quadrennial Homeland Security Review
- Contributed to the revision of several of the 2010 NIPP Sector-Specific Plans (SSPs)
- Contributed to Level 1 and Level 2 criteria lists
- Submitted to the Assistant Secretary a white paper entitled, *Aligning Federal CIKR Capabilities to Meet Needs in the Field*
- Sponsored a variety of landscape studies, effective practice guides and state sunshine law documents and disseminated to the SLTT community
- Supported the implementation of the Alliance Networks for more effective communications between DHS and the critical infrastructure owners and operators
- Enhanced the SLTTGCC HSIN portal for information-sharing between Federal, SLTT governments and the private sector
- Helped ensure the development and implementation of actionable national critical infrastructure policies

SLTTGCC MEMBERS

- Alabama Department of Homeland Security
- Alaska Division of Homeland Security and Emergency Management
- Arizona Department of Homeland Security
- Bloomington, Minnesota Fire Department
- California Emergency Management Agency
- City of East Providence, Rhode Island
- City of Seattle, Washington
- Colorado State Police, Office of Preparedness and Security
- Commonwealth of Puerto Rico
- Hennepin County, Minnesota Department of Human Services and Public Health
- Hualapai Nation Police Department
- Maine Emergency Management Agency
- Massachusetts Office of Homeland Security
- Miami Nation
- Michigan State Police
- Nassau County, New York Department of Health, Office of Public Health Preparedness
- New Jersey Office of Homeland Security
- New York State Office of Homeland Security

- Reviewed and provided comments on the White House Surface Transportation Security Priority Assessment

Key Initiatives

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

Key initiatives within the council include the following:

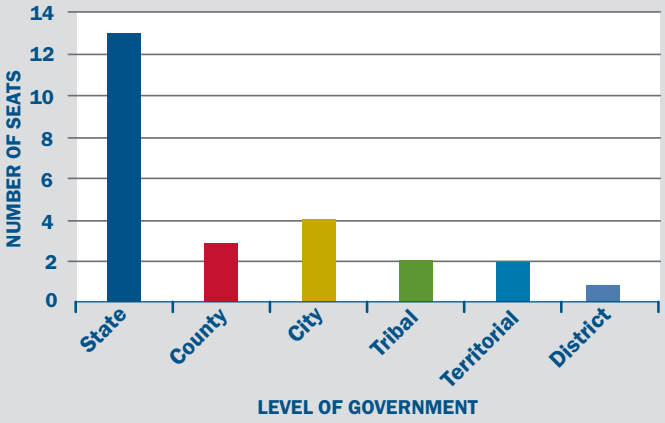
- Encouraging and facilitating State and local implementation of the NIPP through the expanded use of ACAMS and other automated collection and analysis tools
- Developing a process for accessing Chemical-terrorism Vulnerability Information that provides the appropriate level of security safeguards while allowing the effective, efficient transfer of crucial preparedness information to State and local homeland security partners
- Conducting aggressive outreach efforts with SLTT constituents to increase the number of individuals using the SLTT portal, so that more information can be shared between the Council and constituents
- Strengthening the incorporation of critical infrastructure intelligence information requirements within the intelligence cycle of non-Federal fusion centers
- Participating in national plan review efforts, including the triennial review of the NIPP, its associated SSPs, and critical infrastructure annexes
- Identifying baseline characteristics of regional consortiums for critical infrastructure protection and effective practices in the formation of regional, State-based critical infrastructure protection organizations

Path Forward

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

- Broaden its pool of members and subject matter experts
- Encourage the integration of a regional perspective into the NIPP partnership framework
- Advocate consensus-built requirements to address gaps in information sharing
- Ensure effective and efficient liaisons with the critical infrastructure sector councils
- Continue to evaluate the Homeland Security Information Network as the communications vehicle
- Continue to focus on the full integration of the NIPP into an all-hazards environment

SLTTGCC Member Representation



The graph above demonstrates the diversity of representation within the SLTTGCC.

"The [State, Local, Tribal, and Territorial Government Coordinating Council] provides the U.S. Department of Homeland Security with the diverse, proven, real-world experience that improves the relevance of policies and the effectiveness of programs."

Source: 2010 SLTTGCC Annual Report

"[Automated Critical Asset Management System] 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 [critical infrastructure] protection programs."

Source: 2010 SLTTGCC Annual Report

"The [State, Local, Tribal, and Territorial Government Coordinating] Council continues to collaborate with the Federal intelligence and analysis community to integrate [critical infrastructure] protection into State and [Urban Areas Security Initiative] fusion centers."

Source: 2010 SLTTGCC Annual Report

- Oklahoma Office of Homeland Security
- Southern Nevada Health District
- St. Clair County, Michigan, Department of Emergency Management/Homeland Security
- St. Louis, Missouri, Office of Emergency Services
- Utah Department of Public Safety
- Virgin Islands Office of Homeland Security
- Virginia Governor's Office of Commonwealth Preparedness

REGIONAL CONSORTIUM COORDINATING COUNCIL

Partnership

Regional critical infrastructure partnerships involve multijurisdictional, 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 the implementation of the National Infrastructure Protection Plan (NIPP) at the regional level, DHS recognized the Regional Consortium Coordinating Council (RCCC) in July 2008, as a self-organized, self-governed body focused on addressing regional challenges in implementing the National Infrastructure Protection Plan (NIPP). These activities may include enhancing physical, cyber, and personnel security of infrastructure; emergency preparedness; and overall industrial and governmental continuity and resilience of one or more States, urban areas, or municipalities. Currently, the RCCC has 14 members that represent 30 States and nine metropolitan areas. 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 resilience of critical infrastructures nationwide.

Goals

The RCCC has identified the following security goals:

- Sponsor or support cooperative public-private regional 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 and local homeland security partners, DHS, the sectors within the Critical Infrastructure Protection Advisory Council (CIPAC), and its cross-sector councils
- Support DHS and critical infrastructure sector partnership communication, and coordination of homeland security risk mitigation and vulnerability assessment initiatives involving members of the regional consortium entities within the RCCC
- Assist in identifying requirements for the coordination and efficient allocation of regional and local critical infrastructure private sector security clearances among private sector critical infrastructure within specific regions as required by DHS
- Work with Federal, State, and local government agencies to properly integrate critical infrastructure-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
- Foster ongoing coordination with DHS, State and local governments, and the critical infrastructure 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 preparedness of regional consortia and their member entities and incorporate them, as appropriate, into a Council inventory that is accessible and available to all RCCC member entities
- 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

Recent accomplishments of the RCCC include the following:

- Established and routinely updated the Homeland Security Information Network – Critical Sectors (HSIN-CS) portal to communicate unclassified threats, report on incidents, and share best practices
- Sponsored the regional ports security workshop
- Created a public Web site, **www.r-ccc.org,** which will serve as the primary outreach mechanism for the council

RCCC MEMBERS

- Alaska Partnership for Infrastructure Protection
- All Hazards Consortium
- California Resiliency Alliance
- ChicagoFIRST
- Colorado Emergency Preparedness Partnership
- Dallas-Fort Worth FIRST
- InfraGard Los Angeles
- Mid-America Business Force
- New Jersey Business Force
- Pacific Northwest Economic Region
- Safeguard Iowa
- Southeast Emergency Response Network
- South East Regional Research Initiative
- U.S. Chamber of Commerce

Key Initiatives

The RCCC is engaged in various initiatives to advance critical infrastructure protection, vulnerability reduction, and consequence mitigation.

Key initiatives within the RCCC include the following:

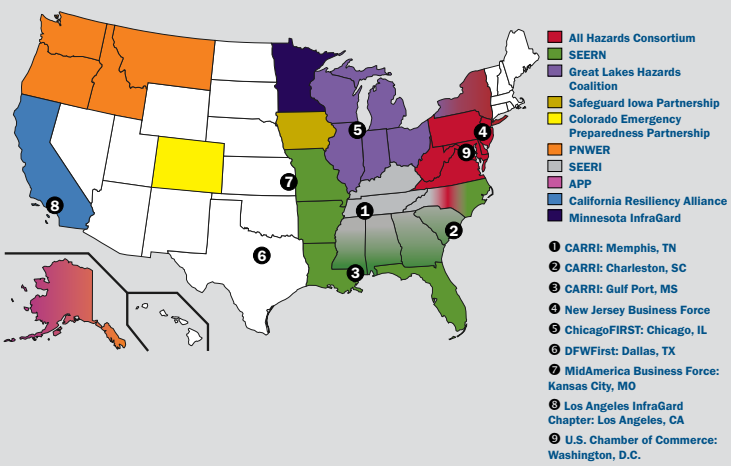
- Developing a critical infrastructure regional resilience roadmap to advance coordination and participation within and among regions to improve critical infrastructure resilience
- Creating a nationwide compendium of regional organizations that are active in critical infrastructure protection and resilience
- Establishing a series of workshops that brings in maximum numbers of regional stakeholders to generate outcomes that further the RCCC mission
- Encouraging State 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 decisionmaking

Path Forward

The RCCC has developed an aggressive plan to accelerate its maturation throughout 2010 and 2011. Steps that will be taken as the RCCC moves forward in achieving its goals include the following:

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

Regional Consortium Coordinating Council Map of Participants



"During 2009 and in the beginning of 2010, the RCCC continued to develop its operating structure while initiating projects focused on regional protection and resilience."

Source: 2010 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."

Source: 2010 Regional Consortium Coordinating Council Annual Report

"The RCCC provides a unique mechanism to integrate National Infrastructure Protection Plan implementation on a regional scale, thereby accelerating the rate and increasing the depth of overall nationwide protection and resilience."

Source: 2010 Regional Consortium Coordinating Council Annual Report

BANKING AND FINANCE SECTOR

Partnership

The Banking and Finance Sector is essential to facilitating world economic activity. The partnership's private sector members include the Financial Services Sector Coordinating Council (FSSCC) for Critical Infrastructure Protection and Homeland Security; the Financial Services Information Sharing and Analysis Center (FS-ISAC); and the Regional Partnership Council Financial Industry Resilience, Security, and Teamwork (RPC*first*). 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 manmade disasters. FS-ISAC was 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 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 Treasury Department will work together to achieve the following sector-specific goals:

- Achieve the best possible position in the face of a myriad of intentional, unintentional, manmade, and natural threats against the sector's physical and cyber infrastructure
- Address and manage the risks posed by the dependence of the sector on the Communications, Information Technology, Energy, and Transportation Systems Sectors
- Work with the law enforcement community, financial regulatory authorities, private sector, and international counterparts

Selected Accomplishments

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

- Created the Financial Services threat matrix that evaluates threats across all organization types, macro functions, and business processes, resulting in more than 1,900 unique combinations
- Published the *Resilient International Telecommunications Guidelines for the Financial Services Sector*
- Expanded research and development on the top priorities including focused collaboration with academia and the Federal Government on improving identity validation and developing a financial communications and authentication pilot
- Expanded cybersecurity capabilities to address emerging needs in supply chain and identity management, including significant contributions to the National Strategy for Trusted Identities in Cyberspace
- Strengthened partnership throughout the sector
- Launched the Government Information Sharing Framework initiative pilot program

Key Initiatives

Sector protective program initiatives aim to achieve the aforementioned sector goals through several key initiatives, including the following:

- Identifying, prioritizing, and developing mitigation and protection strategies and initiatives against significant sector threats, incidents, and vulnerabilities through the development of the threat matrix
- Participating in Department of Homeland Security (DHS) cyber-based training such as the Cyber Financial Industry and Regulators Exercises, which included FSSCC, FS-ISAC, RPC*first*, U.S. Secret Service, Federal Bureau of Investigation, and DHS
- 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 sectors and appropriate government agencies to address critical interdependencies, including telecommunications diversity and resilience and electrical power grid vulnerabilities

FBIIC MEMBERS

- 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 Credit Union Administration
- Office of the Comptroller of the Currency
- Office of Thrift Supervision
- Securities and Exchange Commission
- Securities Investor Protection Corporation
- U.S. Department of the Treasury

FSSCC MEMBERS

- American Bankers Association
- American Council of Life Insurers
- American Insurance Association
- BAI
- Bank of America
- Bank of NY/Mellon
- Barclays
- BITS/The Financial Services Roundtable
- CME Group
- ChicagoFIRST
- Citigroup
- The Clearing House
- CLS Group
- Consumer Bankers Association
- Credit Union National Association
- The Depository Trust & Clearing Corporation
- Fannie Mae

- Meeting with and continuing to build relationships with representatives from other sectors through the Partnership for Critical Infrastructure Security

Path Forward

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

- Understand top threats to the sector through developing the Banking and Finance Sector threat matrix and updating sector priorities and strategies
- Participate in regional and national exercises to test and enhance the resilience of the sector
- Encourage 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 the law enforcement community to share information on cybersecurity threats that may directly or indirectly impact the sector and develop strategies to reduce the potential impact on sector operations
- Coordinate with DHS to sponsor classified-level clearances for need-to-know personnel within the sector to facilitate the sharing of relevant information affecting the sector
- Coordinate crisis response by facilitating the timely dissemination of critical information within the sector and among sector constituencies and other affected parties
- Support a private sector research and development initiative to explore ways to make the Banking and Finance Sector's systems more resilient against cyber threats

"Addressing the emerging important topics in cyber security, two new working groups were created in 2009, the Identity Management Working Group and the Supply Chain Working Group.""

Source: 2010 Banking and Finance Sector Annual Report

"Cyber Financial Industry and Regulators Exercise is part of a long-running, robust effort by the financial sector to address the cyber-based risks and vulnerabilities that stem from the sector's dependence on information and communications infrastructure"

Source: 2010 Banking and Finance Sector Annual Report

- 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 Association of Insurance Commissioners
- National Association of State Credit Union Supervisors
- National Futures Association
- Navy Federal Credit Union
- North American Securities Administrators Association
- 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, Office of Infrastructure Protection (IP). Within IP, responsibilities for Chemical Sector protection and resilience are held by two divisions. The Sector-Specific Agency Executive Management Office Chemical Branch has responsibility for overseeing voluntary efforts by serving as the Sector-Specific Agency (SSA) for the Chemical Sector. The Infrastructure Security Compliance Division was established to administer regulatory activities.

A fundamental objective of the 2009 National Infrastructure Protection Plan (NIPP) is to protect and improve the resilience of infrastructure identified as critical. As one of the oldest industries in the country, the chemical industry has a long history of resilience based on the sector's ability to adapt to, prevent, prepare for, and recover from all hazards, including natural disasters, fluctuating markets, or changes in regulatory programs. To maintain operational resilience, successful businesses identify their critical dependencies and interdependencies and develop appropriate strategies to manage disruptions in critical systems should they occur.

Partnerships in the Chemical Sector have matured along with programs intended to strengthen the sector's protective posture. The industry implements a variety of voluntary security programs and continues to make significant capital investments to address security concerns. Several States also adopted measures to enhance security of chemical facilities under their jurisdiction. While acknowledging industry and State efforts to secure chemical facilities, the Federal Government continues to implement security regulations at sites it deems high risk to ensure a uniform approach to security.

Vision

An economically competitive and increasingly resilient industry that achieves and maintains a sustainable security posture by effectively reducing vulnerabilities and consequences of all hazards, using risk-based assessments, industry best practices, and a comprehensive information-sharing environment between industry and government.

Goals

Sector goals and objectives were revised to consider all hazards, incorporate a greater focus on resilience, address cybersecurity, and ensure greater alignment with sector programs and activities. The overarching goals of the sector include the following:

- Evaluate the security posture of Chemical Sector high-risk assets including physical, cyber, and human elements as needed
- Prioritize Chemical Sector critical infrastructure protection activities based on risk
- Sustain risk-based, cost-effective sector-wide protective programs that increase asset-specific resilience without hindering the economic viability of the sector
- Refine processes and mechanisms for ongoing government and private sector coordination to increase sector resilience, as necessary
- Support risk-based critical infrastructure protection R&D projects that add value to the Chemical Sector
- Measure the progress and effectiveness of sector critical infrastructure protection activities

Selected Accomplishments

Sector partners continue to maintain and enhance the protective posture of the Chemical Sector. Notable accomplishments over the past year include the following:

- Covered 4,895 facilities as of August 30, 2010 with Chemical Facilities Anti-Terrorism Standards (CFATS), and assigned more than 4,100 facilities to a final tier, leaving 795 awaiting assignment to a final tier
- Conducted the fourth annual Chemical Sector Security Summit in July 2010, drawing a record attendance of 400 people with 75 percent of attendees representing industry
- Developed and finalized the *2010 Chemical Sector-Specific Plan* through collaborative efforts by the Sector Coordinating Council (SCC), SSA, and Government Coordinating Council (GCC)
- Adopted Sector-Specific Metrics tailored for SCC members at the corporate-level. Through a web-based survey tool, survey respondents reported they are actively engaged in assessing risk, integrating security into both emergency response and business continuity plans, and making good progress in securing critical cyber assets
- Increased attendance by 88 percent at this year's six Chemical Sector Explosives Threat Awareness Trainings (CSETAT)
- Supported tabletop exercises in Pennsylvania, New Jersey, California, Missouri, Ohio, New York, and Louisiana
- Developed two best practices documents designed to reduce risk at facilities—*DHS Chemical Sector Security Awareness Guide*, and *Chemical Facility Security: Best Practices Guide for an Active Shooter*

GCC MEMBERS

- Chemical Safety Board
- Office of the Director of National Intelligence
- State, Local, Tribal, and Territorial Government Coordinating Council
- 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. Environmental Protection Agency

- Developed the *Chemical Sector Training Resources Guide* to assist facility security officers train their employees on industry best practices, physical security and cybersecurity awareness, and emergency management and response
- Continued information-sharing efforts to include four classified briefings for the private sector, during which the intelligence community provided briefings on both physical and cyber threats
- Certified nearly 5,000 individuals from 415 companies as completing its Web-based Chemical Security Awareness Training Program since it was launched in July 2008

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 CFATS
- Improving security practices and raising awareness through private sector security guidance programs, documents, and plans
- Developing and promoting free, Web-based tools, training, and best practices documents for easy access by all sector partners
- Enhancing information sharing through the Chemical Sector Security Summit, the Classified Sector Briefings, monthly suspicious activity teleconferences, and the Homeland Security Information Network
- Raising awareness by providing educational training opportunities, such as CSETAT and Web-based Chemical Security Awareness Training for Chemical Sector security professionals and other sector partners
- Promoting the Voluntary Chemical Assessment Tool so facilities can conduct effective cost-benefit analyses of security measures
- Expanding participation in the research and development process through the SCC Research and Development Working Group
- Implementing the *Roadmap to Secure Control Systems in the Chemical Sector*

Path Forward

Numerous steps will be taken as the Chemical Sector moves forward in protecting and enhancing the resilience of its critical infrastructure. These steps may include the following:

- Encourage an ongoing private-public dialogue through the NIPP partnership framework to improve information sharing on chemical security legislation and the efforts to harmonize security regulations across the Federal Government
- Maximize outreach efforts to owners and operators, state chemical industry councils, and first responder communities to introduce their members to free SSA-sponsored programs
- Continue to engage owners and operators throughout the sector on the importance of integrating physical security and cybersecurity

"The Chemical Sector has a long history of its own security programs and has taken a lot of initiative of its own accord. I want to applaud you for these efforts; they illustrate a fundamental point about homeland security and the role of the private sector."

Source: DHS Secretary Janet Napolitano at the 2010 Chemical Sector Security Summit

"Information provided is practical and actionable. Please continue this in future Summits."

Source: 2010 Chemical Sector Security Summit Attendee on the Active Shooter Breakout Session

"Excellent overview. I appreciated the material and opportunities to ask questions. I would recommend this to others."

Source: Participant at a Chemical Sector Explosives Threat Awareness Training

"This was worth the time out of the office. Thought provoking to make improvements with best practices and confirmed we are doing some things correctly...Thank you!"

Source: Participant at a Chemical Sector Explosives Threat Awareness Training

SCC MEMBERS

- Agricultural Retailers Association
- American Chemistry Council
- American Coatings Association
- BASF
- Chemical Producers and Distributors Association
- The Chlorine Institute
- Compressed Gas Association
- CropLife America
- The Fertilizer Institute
- Institute of Makers of Explosives
- International Institute of Ammonia Refrigeration
- International Liquid Terminals Association
- National Association of Chemical Distributors
- National Petrochemical and Refiners Association
- Rhodia
- Society of Chemical Manufacturers & Affiliates
- Terra Industries, 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 differing needs and challenges. The Commercial Facilities Sector also includes facilities and assets (e.g., sporting stadiums, entertainment districts, and amusement and theme parks) that host activities which 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 (DHS) 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 a favorable business environment conducive to attracting and retaining employees, tenants, and customers.

Goals

DHS and Commercial Facilities Sector partners have identified eight overarching goals to improve the protective posture of the sector:

- Enable trusted and protected information sharing between partners at all levels of government
- Ensure that the public sector security partners disseminate timely, accurate, and threat-specific information and analysis throughout the sector
- Preserve the "open access" business model of most commercial facilities while enhancing overall security
- Maintain a high level of public confidence in the security of the sector
- Provide security that meets the needs of the public, tenants, guests, and employees while ensuring the continued economic vitality of the owners, investors, lenders, and insurers
- Have systems in place (e.g., emergency preparedness, training, crisis response, and business continuity plans) to ensure a timely response to and recovery from natural or 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

Both private and public partners in the Commercial Facilities Sector have made numerous accomplishments in bolstering sector protection and resilience. Some of the sector's accomplishments over the past year include the following:

- Created protective measures guides for U.S. lodging, outdoor events, mountain resorts, credentialing, and bag searches
- Produced pandemic influenza planning documents for public assembly facility owners
- Developed three new programs with the National Center for Spectator Sports Safety and Security and continued implementation of seven existing programs
- Continued to make progress in establishing a National Sports Security Laboratory
- Created a National Basketball Association (NBA) Arena Audit Program and implemented emergency evacuation plans at NBA arenas
- Increased awareness of National Cyber Security Division resources by conducting one-on-one meetings with partners, presenting at industry conferences, and conducting other outreach
- Implemented a new Subsector Outreach and Information Sharing Initiative focused on tabletop exercises, protective security advisor visits, and new product development, including training and awareness videos for the Lodging, Retail, and Sports Leagues Subsectors

GCC MEMBERS

- National Endowment for the Arts
- U.S. Department of Agriculture
- U.S. Department of Education
- U.S. Department of Health and Human Services
- U.S. Department of Homeland Security
- U.S. Department of the Interior
- U.S. Department of Justice
- U.S. Department of State
- U.S. Environmental Protection Agency

SCC MEMBERS

- Affinia Hospital
- Beacon Capital
- BOMA International
- Cushman and Wakefield
- Dallas Convention Center
- International Association of Amusement Parks and Attractions
- International Association of Assembly Managers
- International Association of Fairs and Exhibitions
- International Council of Shopping Centers
- The Loss Prevention Foundation
- Major League Baseball

Key Initiatives

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

- Providing explicit risk mitigation guidance to owners and operators through DHS hotel and lodging advisory posters, protective measures guides, *Active Shooter – How to Respond* training materials, pandemic influenza planning documents for public assembly facilities, Building Owners and Managers Association international awareness programs, and the Commercial Facilities Sector-Specific Agency outreach program
- Fostering an educational framework in which risk methodologies can be explored and understood for the purposes of training through programs offered by the National Center for Spectator Sports Safety and Security and classes offered by the International Association of Assembly Managers Academy for Venue Safety and Security
- Expanding the use of the Risk Self-Assessment Tool (RSAT) for Stadiums and Arenas, which offers arenas and stadiums the capability to balance resilience with focused, risk-informed prevention, protection, and preparedness activities
- Strengthening both the international supply chain and U.S. Border Security through the Customs-Trade Partnership Against Terrorism
- Encouraging the development and deployment of new and innovative anti-terrorism 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 protecting and enhancing the resilience of its critical infrastructure. These steps include the following:

- Develop additional modules for RSAT and more protective measures guides that focus on different subsectors
- Work with private and governmental partners for subsector outreach and information-sharing initiatives through tabletop exercises, concentrating on subsectors that have not yet been the focus of the initiative
- Continue to highlight the importance of cybersecurity by engaging with sector partners through numerous forums, such as the Cross-Sector Cybersecurity Working Group and the National Strategy for Trusted Identities in Cyberspace
- Place greater emphasis on resilience and interdependencies by employing the Regional Resilience Assessment Program, which evaluates regional critical infrastructure to identify dependencies, interdependencies, cascading effects, resilience characteristics, and gaps

"There is a 100 percent graduation rate for all students attending the Academy for Venue Safety and Security training course."

2010 Sector Annual Report: Commercial Facilities Sector

"In 2009, there were 27 reported incidents of 'fans entering the field of play…This is a 47 percent reduction from the 57 percent reported field intrusions in 2007."

2010 Sector Annual Report: Commercial Facilities Sector

"All 29 National Basketball Association arenas (100%) have developed emergency evacuation plans."

2010 Sector Annual Report: Commercial Facilities Sector

- Marriott International
- NASCAP, 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
- Paramount
- RBC Center
- Real Estate ISAC
- Related Management Company
- Retail Industry Leaders Association
- Self Storage Association
- Stadium Managers Association
- Starwoods Hotel and Resorts
- The Real Estate Roundtable
- Tishman Speyer Properties
- The Walt Disney Company
- Trump Corporation
- Warner Brothers Studio Facilities
- Westfield Shopping Centers

COMMUNICATIONS SECTOR

Partnership

The Communications Sector includes wireline, wireless, satellite, cable, and broadcasting industries as well as the transport networks that support the Internet and other key information systems. The Communications Sector has a long history of cooperation among its members and with the Federal Government with respect to national security/emergency preparedness (NS/EP) communications. This history distinguishes the Communications Sector from most other critical sectors identified in the National Infrastructure Protection Plan. The sector personifies cooperation and trusted relationships that have resulted in the delivery of critical services when emergencies and disasters occur. Forty-five private sector organizations and their respective trade associations form the Communications Sector Coordinating Council (SCC), and 12 Federal departments and their agency members form the Communications Government Coordinating Council (GCC). The National Communications System (NCS) within DHS serves as the Sector-Specific Agency and also manages the National Coordinating Center for Communications (NCC and the Network Security Information Exchange). These are just two examples of sector partnerships that provide government and industry response coordination and information-sharing mechanisms.

Vision

The United States has a critical reliance on assured communications. The Communications Sector strives to ensure that the Nation's communications networks and systems are secure, resilient, and rapidly restored in the event of disruption.

Goals

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

- Protect and enhance the overall physical and logical health of communications
- Reconstitute critical communications services rapidly in the event of disruption and mitigate cascading effects
- Improve the sector's NS/EP posture with Federal, State, local, tribal, international, and private sector entities to reduce risk

Selected Accomplishments

Public and private sector 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:

- Established the 2011 National Sector Risk Assessment (NSRA) Working Group consisting of government and industry partners who will develop the 2011 NSRA
- Coordinated input from the National Security Telecommunications Advisory Committee for the White House Report on The National Strategy for Trusted Identities in Cyberspace
- Celebrated over 25 years of government-industry partnerships through the NCC
- Launched the National Cybersecurity and Communications Integration Center to enable a unified response capability for the Communications and IT Sectors
- Established the Telecom / Energy working group to mitigate long-term power outages
- Completed the 2010 Communications Sector-Specific Plan (SSP) and Sector Annual Report
- Coordinated and published the National Security Information Exchange Assessment of the Risk to the Cybersecurity of the Public Network
- Conducted a week-long workshop and training exercise involving Federal emergency and private sector communications personnel in support of Emergency Support Function #2

Key Initiatives

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

Key initiatives within the sector include the following:

- Completing the 2011 NSRA
- Developing more efficient communications capabilities through government-to-government priority telecommunications services via the Government Emergency Telecommunications Service and NS/EP functions

GCC MEMBERS

- Federal Communications Commission
- Federal Reserve Board
- General Services Administration
- National Association of Regulatory Utility Commissioners
- National Telecommunications and Information Administration
- Nuclear Regulatory Commission
- State, Local, Tribal, and Territorial Government Coordinating Council
- 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
  - Federal Bureau of Investigation
- U.S. Department of State

SCC MEMBERS

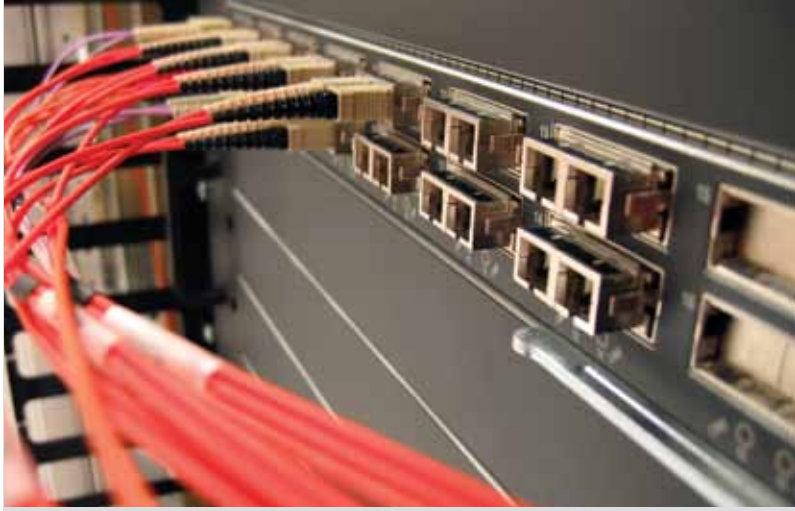
- 3U Technologies
- Alcatel-Lucent
- AmeriCom-GS
- Association of Public Television Stations
- AT&T
- Boeing
- Century Link
- CTIA - The Wireless Association
- Cincinnati Bell
- Cisco Systems
- Comcast
- Computer Sciences Corporation
- Digi International
- DirecTV
- Harris Corporation
- Hughes Network Systems
- Internet Security Alliance

- Increasing the number of subscribers to the Telecommunications Services Priority program, which is a regulatory, administrative, and operational system authorizing and providing for priority treatment of telecommunications services
- Enhancing information sharing and situational awareness through the Network Security Information Exchange, a forum to share data about vulnerability in public telephone networks
- Participating in National Level Exercises and training to test and improve response and recovery capabilities

Path Forward

The sector will continue planning for the implementation of the 2010 Communications SSP. Activities within the plan include the following:

- Continue to develop next-generation network priority services to meet the evolving requirements of critical communications customers in a converged communications environment
- Develop a Communications Sector outreach program to educate Communications Sector customers and other infrastructure owners and operators about communications infrastructure resilience and risk management practices
- Develop educational programs on communications technologies and their potential points of failure during emergencies
- Develop a detailed quantitative risk assessment to identify and prioritize portfolios of countermeasures to mitigate the impacts of bulk power outages on key communications infrastructure
- Improve mechanisms to collect, aggregate, analyze, visualize, and share cyber risk information between the Communications and IT Sectors
- Examine specific backup alternative electrical power solutions, such as hybrid photovoltaic fuel cell power sources, to support NS/EP communications as part of a revised NCS Manual 3-10-1, *Guidance for Implementing NCS Directive 3-10, Minimum Requirements for Continuity Communications Capabilities*
- Continue to develop and strengthen Communications Sector interdependency relationships with other critical infrastructure partners



"The American Recovery and Reinvestment Act of 2009 appropriated funds and granted the U.S. Department of Agriculture's Rural Utilities Services and the U.S. Department of Commerce's National Telecommunications and Information Administration the authority to expand access to broadband services in the United States."

Source: 2009 Communications Sector Annual Report

"During the reporting period, the [National Security Telecommunications Advisory Committee] also undertook its first classified effort, working directly with the Executive Office of the President (EOP) and provided comments on the EOP's draft *National Strategy for Secure Online Transactions*."

Source: 2009 Communications Sector Annual Report

"During the last year, 237 new organizations participated in the [Telecommunications Service Priority] program for the first time. This is an increase of 95 new users from 2008."

Source: 2009 Communications Sector Annual Report

- Intrado, Inc.
- Iridium
- Juniper Networks
- Level 3
- McLeodUSA
- Motorola
- National Association of Broadcasters
- National Cable & Telecommunications Association
- Neustar
- Nortel
- Powerwave
- Qwest
- Research in Motion
- 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
- U.S. Internet Services Provider Association
- U.S. Telecom Association
- Utilities Telecom Council
- 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 contributed $676 trillion to the U.S. economy. The Critical Manufacturing Sector Coordinating Council (SCC) currently includes representatives from 23 manufacturing companies and the Critical Manufacturing Sector Government Coordinating Council (GCC) includes representatives from 12 Federal departments and agencies and the State, Local, Tribal, and Territorial GCC. The U.S. Department of Homeland Security (DHS), Office of Infrastructure Protection is the Sector-Specific Agency (SSA) for the Critical Manufacturing Sector.

Vision

To reduce risks to the Critical Manufacturing Sector through proactive prevention of, preparation for, and mitigation of natural and manmade threats, leading to effective response and recovery through public-private partnership.

Goals

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

- Achieve an understanding of the assets, systems, and networks that compose 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 resilience 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 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 measures over the past year to increase the sector's security and resilience, including the following:

- Expanded the membership of the Critical Manufacturing SCC and GCC
- Worked with sector partners to define sector goals and objectives and developed the Critical Manufacturing Sector-Specific Plan
- Collaborated with the Defense Industrial Base Sector and National Cyber Security Division to assess risks posed to certain manufacturing facilities
- Fostered enhanced partnerships through information sharing

Key Initiatives

Sector partners, both public and private, engage in a wide variety of activities to mitigate risks to critical infrastructure. These activities enable the sector to further enhance its protective posture.

Key initiatives within the sector include the following:

- 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 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
- Developing a regional network of the SCC comprised of all-sized manufacturers that form a true representation of the sector
- Increasing information sharing by using the Homeland Security Information Network-Critical Sectors (HSIN-CS) and enhance the HSIN-CS Critical Manufacturing portal

GCC MEMBERS

- Small Business Administration
- State, Local, Tribal, and Territorial Government Coordinating Council
- 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
  - Federal Bureau of Investigation
- 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

Path Forward

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

- Develop a working group to discuss the sharing of relevant classified and unclassified information
- Develop a working group to identify gaps in information sharing between public and private Critical Manufacturing Sector partners
- Continue expansion and enhancement of the HSIN-CS Critical Manufacturing portal
- Increase involvement of the State and local communities
- Regionalize the SCC

"Given the size and diversity of the CM [Critical Manufacturing] Sector, there is no universal solution to implementing protective security measures. Protective measures currently implemented within the CM Sector span the elements of the National Infrastructure Protection Plan Risk Management Framework and address physical, cyber, and human dimensions."

Source: 2010 Critical Manufacturing Sector Annual Report

"[The Critical Manufacturing Sector Coordinating Council] increased its membership by 100% in 2009, bringing its membership count from 10 to 20 partners."

Source: 2010 Critical Manufacturing Sector Annual Report

"The Cyber Exercise Program will achieve an understanding of the assets, systems, and networks that comprise the critical infrastructure of the [Critical Manufacturing] Sector and develop processes for ensuring appropriate and timely information sharing between government and private sector partners in the Critical Manufacturing Sector."

Source: 2010 Critical Manufacturing Sector Annual Report

SCC MEMBERS

- ArcelorMittal USA
- Boeing
- Bridgestone Americas, Inc.
- Carpenter Technology Corporation
- Caterpillar Inc.
- Chrysler LLC
- Cisco Systems, Inc.
- Delphi
- Emerson
- Ford Motor Company
- General Electric
- General Motors Company
- Goodyear Tire & Rubber Company
- Intel Corporation
- ITT Corporation
- John Deere
- Kohler Company
- Navistar International Corporation
- Nichols Brothers Boat Builders
- Oshkosh Corporation
- Penske
- Remy International
- Schweitzer Engineering Laboratories, Inc.
- Smith and Wesson
- United Technologies Corporation
- U.S. Steel Corporation
- Whirlpool Corporation

DAMS SECTOR

Partnership

The Dams Sector is comprised of dam projects, navigation locks, levees, hurricane barriers, mine tailings impoundments, and other similar water retention and 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 more than 82,000 dams in the United States; approximately 65 percent are privately owned and more than 85 percent are regulated by State dam safety offices. The Dams Sector operates under the auspices of the Critical Infrastructure Partnership Advisory Council framework, and 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 is the Dams Sector-Specific Agency and 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 multi-faceted, multi-level, and flexible protective programs and resilience 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 and resilience-enhancing technologies, will ensure the continued economic use and enjoyment of this key resource through a risk-informed management framework addressing preparedness, response, mitigation, and recovery.

Goals

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

- Build Dams Sector partnership and improve communications among all critical infrastructure partners
- Identify Dams Sector composition, consequences, and critical assets
- Improve the Dams Sector's understanding of viable threats
- Identify Dams Sector vulnerabilities
- Identify risks to Dams Sector critical assets
- Develop guidance on how the Dams Sector will manage risks
- Enhance security and resilience 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 protection and resilience. Some of the sector's accomplishments over the past year include the following:

- Developed the *Roadmap to Secure Control Systems in the Dams Sector*
- Implemented the Dams Sector Suspicious Activity Reporting tool
- Developed comprehensive Web-based training courses on security awareness, protective measures, and crisis management
- Conducted 2009 Dams Sector Exercise Series
- Developed the portfolio prioritization tool to rank critical assets by potential consequence severity
- Continued implementing the Consequence-Based Top Screen methodology online tool to identify critical sector assets

Key Initiatives

The Dams Sector has a number of initiatives to enhance the protection and resilience of the Nation's dams and related infrastructure. Some of these initiatives include the following:

- Developing improved blast-induced damage analysis capabilities and simplified damage estimation models
- Identifying and characterizing Dams Sector assets and providing a sector-wide prioritization framework
- 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

GCC MEMBERS

- Commonwealth of Virginia, Department of Conservation and Recreation
- Federal Energy Regulatory Commission
- International Boundary & 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 Virginia, Department of Conservation and Recreation
- State of Washington, Department of Ecology
- Tennessee Valley Authority
- U.S. Army Corps of Engineers
- 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 the Interior
- U.S. Department of Labor
- U.S. Department of State
- U.S. Environmental Protection Agency

- Developing and widely distributing technical reference handbooks, guides, brochures, and training materials
- Developing guidance aimed at strengthening cybersecurity within the Dams Sector

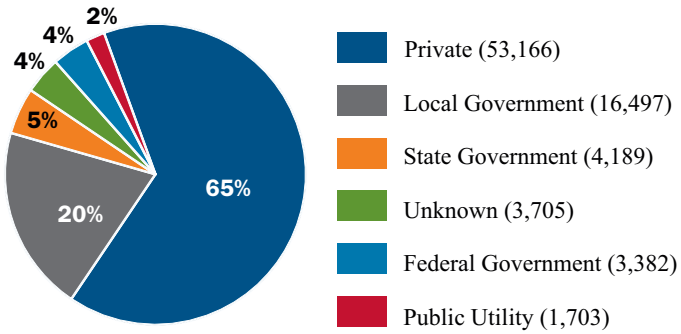
Path Forward

The Dams Sector faces the following challenges at it continues to develop and implement security-related programs for its assets: cybersecurity, information sharing, funding constraints, and infrastructure condition. To address these challenges, the Dams Sector will take the following steps:

- Compile lessons learned from the challenges associated with the implementation of the existing cybersecurity regulatory standards
- Continue to safeguard facility-sensitive information from disclosure
- Continue to identify and characterize critical assets in an effort to demonstrate the need for a risk-based, multi-year, and multi-jurisdictional infrastructure rehabilitation program
- Increase reliance on the Homeland Security Information Network by enabling virtual participation in sector quarterly councils and workgroup meetings

Dams Ownership Structure

National Inventory of Dams-listed Assets



"The Dams Sector successfully completed and implemented the Consequence-Based Top Screen methodology to assist sector stakeholders in identifying and characterizing the subset of high-consequence facilities whose failure or disruption could potentially lead to the most severe impacts."

Source: 2010 Dams Sector Annual Report

"The 2009 Dams Sector Exercise Series – Columbia River Basin (DSES-09) was conducted by the U.S. Department of Homeland Security (DHS), USACE, and the Pacific Northwest Economic Region (PNWER), in collaboration with multiple public and private stakeholders across the region. DSES-09 involved a severe rain-on-snow event affecting a large portion of the Columbia River Basin causing overtopping and subsequent breaching of levees in the Tri-Counties area (Benton, Franklin, and Walla-Walla) of southeastern Washington State. The DSES-09 Action Plan provides a roadmap of activities covering the components of the disaster lifecycle: mitigation, steady-state preparedness, emergency response, long-term recovery, and economic resilience. The DSES-09 Integrated Strategy for Regional Resilience outlines a collaborative approach that public and private sector stakeholders within the region can use to mitigate risk and collectively strengthen disaster preparedness and resilience."

Source: 2010 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
- CMS Energy
- Colorado River Energy Distribution Association
- Dominion Resources
- Duke Energy Corporation
- Exelon Corporation
- Hydro-Quebec
- Los Angeles County Department of Public Works
- 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
- Public Utility District 1 of Chelan County (WA)
- Puget Sound Energy
- Salt River Project Water and Power
- SCANA Corporation
- Seattle City Light
- South Carolina Public Service Authority (Santee-Cooper)
- Southern California Edison
- Southern Company Generation
- U.S. Society on Dams
- Xcel Energy Corporation

DEFENSE INDUSTRIAL BASE SECTOR

Partnership

The Defense Industrial Base (DIB) Sector includes hundreds of thousands of domestic and foreign entities and subcontractors that perform work for the Department of Defense (DoD) and other Federal departments and agencies. These firms research, develop, design, produce, deliver, and maintain military weapons systems, subsystems, components, or parts. Defense-related products and services provided by the DIB Sector equip, inform, mobilize, deploy, and sustain forces conducting military operations worldwide. As the Sector-Specific Agency, 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 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

The DIB Sector partnership engages in collaborative risk management activities to eliminate or mitigate unacceptable levels of risk to physical, human and cyber infrastructures, systems, and networks, thus ensuring DoD continues to fulfill its mission. DIB activities support national security objectives, public health and safety, and public confidence.

Goals

The following sector goals were developed in 2008 and help provide the basis for ongoing risk management activities:

- ***Sector Risk Management:*** Use an all-hazards approach to manage the risk-related dependency on critical DIB assets
- ***Collaboration, Information Sharing, and Training:*** Improve collaboration in a shared knowledge environment 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 (Cyber Security/Information Assurance):*** Manage risk to information that identifies or describes characteristics or capabilities of DIB CIKR, or that by its nature would represent a high risk/high impact to the CIKR or 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:

- Issued formal notification to 339 critical assets in the continental United States, and 23 critical assets outside the continental United States are pending Department of State coordination
- Completed 27 awareness visits and 17 on-site assessments
- Established a DIB network that enables the electronic communication of classified voice and data information between DoD and participating DIB partners
- Improved processes for and expansion plans for the DIB Cyber Security/Information Assurance program

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 the following:

- Developing, coordinating, and approving the annual listing of DIB critical infrastructure and notifying asset owners and operators of changes in criticality
- Developing and deploying a risk self-assessment tool
- Establishing and employing business continuity plans for critical infrastructure owner and operator assets

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

- 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:

- Develop a joint business plan among the government and private sector partners, focused on achieving measurable, identifiable results contributing to sector resilience
- Further cooperate with its partners and with sectors that are of critical importance to the DIB Sector, with a focus on interdependencies
- Participate in other related national sector GCCs and working groups; Partnership for Critical Infrastructure Security and other sector SCCs; and in the State, Local, Tribal, and Territorial Government Coordinating Council and regional working groups
- Reevaluate sector risk-mitigation activities and metrics to incorporate the results of the joint business plan
- Resolve the issue to "validate" credentials for granting non-employee vendor access to critical facilities in real-time
- Reduce the number of redundant assessments and better coordinate facility site visits by DoD and DHS
- Increase the involvement of DIB private sector partners with critical asset criteria and the determination and prioritization processes

"DCMA IAC conducted 27 site-specific outreach visits to DIB CIKR during the reporting period, bringing the cumulative total to 158 such visits, or 43% of the currently identified DIB CIKR."

Source: 2010 Defense Industrial Base Sector Annual Report

"The Defense Cyber Investigations Training Academy operating under DC3 has conducted the first cyber forensics course with eligible DIB private sector members enrolled, as authorized by the National Defense Authorization Act for Fiscal Year 2010."

Source: 2010 Defense Industrial Base Sector Annual Report

SCC MEMBERS

- AAI Corporation
- Aerospace Industries Association
- Alliant Techsystems
- The Analytics Science Corporation
- American Society for Industrial Security International
- BAE Systems
- Boeing Company
- Booz Allen Hamilton
- Computer Sciences Corporation
- Defense Security Information Exchange
- DRS Inc.
- 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
- Textron

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 partnership activities and programs appropriate to the sector are those that allow for an inward-focused perspective and maintain the ability of the response community to engage in its mission during an all-hazard event. 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. In the ESS, 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 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 critical infrastructure strategies, activities, policy, and communications within their organizations, across governments, and between governments and sector members. The Emergency Services Sector Coordinating Council (SCC) is a self-organized, self-led body of ESS members that works collaboratively with the SSA and GCC. The SCC is organized through professional associations that represent the five emergency service disciplines: fire and rescue, law enforcement, emergency medical services, emergency management, and public works. The SCC also 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 in the sector.

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 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 support an information-sharing environment that ensures the availability and flow of accurate, timely, and relevant critical infrastructure information and intelligence about terrorist threats, attacks, natural disasters, or other incidents
- ***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, Resilience, and Reconstitution:*** To improve the sustainability and resilience 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:

- Established an information requirements working group
- Launched a pilot Homeland Security Information Network–Critical Sectors–Emergency Services Sector (HSIN-CS-ESS) portal
- Launched a first responder preparedness pilot through a partnership with the Federal Emergency Management Agency, the Los Angeles Fire Department, and IP
- Established the First Responder Coordination Council and the First Responder Research, Development, Testing & Evaluation Working Group by the DHS Science and Technology (S&T) Directorate
- Completed and awaiting publication of the *2010 Triennial Sector-Specific Plan*

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.

GCC MEMBERS

- American Red Cross
- 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 Defense
  - U.S. Northern Command
- U.S. Department of Health and Human Services
- U.S. Department of Justice
  - Federal Bureau of Investigation
- U.S. Department of Transportation
- U.S. Environmental Protection Agency
- U.S. Fire Administration
- U.S. Secret Service

Key initiatives within the sector include the following:

- Leveraging the information-sharing working group to enhance the sector's information-sharing capabilities within ESS and with other critical infrastructure sectors and Federal, State, and local partners
- Enabling government and public and private entities to perform risk assessments of fixed assets, systems, regional systems, and critical assets through the Emergency Services Self-Assessment Tool
- Improving the ability of first responders to serve their communities following large-scale disasters through the development of a Responder and Family Preparedness Technical Assistance Program
- Encouraging the use of the National Hazardous Materials Fusion Center, a Web-based network that facilitates information sharing for emergency responders who are training for and responding to HAZMAT incidents
- Promoting the National Security Association Homeland Security Initiatives training designed to support the capability and capacity of first responders to prevent, plan for, and respond to all-hazards events
- Developing Virtual USA, a voluntary, practitioner-driven, and federally sponsored initiative focused on cross-jurisdictional information sharing and collaboration among the homeland security and emergency management communities

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 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, sustainable efforts to protect the Nation's critical infrastructure
- Develop actionable products for emergency services personnel that reflect of their needs
- Continue to reach out to and build relationships with Federal, State, local, tribal, and territorial critical infrastructure partners to ensure effective coordination of activities among all government agencies, as well as within IP, that impact emergency responders
- Continue to collaborate with the SCC to facilitate appropriate, value-added exercise objectives for the sector

Emergency Services Sector Disciplines

- Law Enforcement
- Fire and Rescue Services
- Emergency Management
- Emergency Medical Services
- Public works

"The IRWG [Investment Review Working Group], a subcommittee of the ISWG [Interagency Sustainability Working Group], is a team of highly experienced practitioners charged with identifying ESS information requirements and developing the HSIN-CS-ESS portal."

Source: 2010 Emergency Services Sector Annual Report

"In the state of Virginia, [Virtual USA] has reduced response times to hazardous material incidents by 70 percent allowing the state to quickly address threats to the health and safety of its citizens."

Source: 2010 Emergency Services Sector Annual Report

"The Commercial Mobile Alert Service Research, Development, Testing & Evaluation Program partnered with the National Academy of Sciences to host a Public Response Workshop April 13–14, 2010. The two-day workshop acted as a forum to bring together experts, researchers, academics, industry representatives, and practitioners in the field of public alerts and warning, specifically in the area of public response to mobile alerts."

Source: 2010 Emergency Services Sector Annual Report

SCC MEMBERS

- American Ambulance Association
- American Public Works Association
- Central Station Alarm Association
- International Association of Chiefs of Police
- International Association of Emergency Managers
- International Association of Fire Chiefs
- National Association of State EMS Officials
- National Emergency Management Association
- National Fire Protection Association
- National Native American Law Enforcement Association
- National Sheriffs' Association
- New York City Fire Department
- North County Fire Protection District, California
- Rescobie Associates
- Securitas Security Services
- Security Industry Association
- Story County, Iowa
- Winchester, Virginia Police

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 partnerships address security issues and share 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, 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, and work to create efficiency and improved coordination throughout the partnership
- Understand key sector interdependencies and collaborate with other sectors to address them, and incorporate that knowledge in planning and operations
- Strengthen partner and public confidence in the sector's ability to manage risk and implement effective security, reliability, and recovery efforts

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:

- Collaborated and successfully completed the triennial review and revision of the Energy Sector-Specific Plan
- Facilitated the high-impact, low-frequency risk workshop by the DOE and the North American Electric Reliability Corporation
- Developed sound working relationships with other critical infrastructure sectors to include Dams, Chemical, Information Technology, Banking and Finance, and Nuclear Reactors, Materials, and Waste
- Developed a metrics pilot program focused on the resilience of the bulk power system
- Developed Secure Supervisory Control and Data Acquisition Communications Protocol in order for asset owners to safeguard serial communications between remote devices and control centers
- Submitted a report, *A Resilient Power Grid: R&D Challenges to Reduce Vulnerabilities in the Modern Electric System,* to the National Science and Technology Council and the Office of Science and Technology Policy

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 resilience issues
- Preparing technical guidelines, guidebooks, notes, training DVDs, and webcasts

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 the Interior
- U.S. Department of State
- U.S. Department of Transportation
- U.S. Environmental Protection Agency

ELECTRICITY SCC MEMBERS

- American Transmission Company
- 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
- Orlando Utilities Commission
- Reliability First Corporation
- Sho-Me Power Electric Cooperative
- Southern Company Services, Inc.
- UIL Holdings Corporation

OIL AND NATURAL GAS SCC MEMBERS

- American Exploration & Production Council
- American Gas Association
- American Petroleum Institute
- American Public Gas Association
- Anadarko Canada Corporation
- Anadarko Petroleum Corporation

- Maintaining, reviewing, and updating security standards
- Supporting emergency preparedness issues, groups, and security forums
- 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 and address these challenges, including the following:

- Build and strengthen existing critical infrastructure protection partnerships
- Facilitate communication and information exchange through the Homeland Security Information Network; the Office of Infrastructure Security and Energy Restoration's secure website, ISERnet; 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

"In November 2009, Department of Energy and North American Electric Reliability Corporation co-sponsored a unique two-day workshop that addressed high-impact, low-frequency risks to the North American bulk power system.."

Source: 2010 Energy Sector Annual Report

"In partnership with DHS, DOS, and DoD, the Office of Infrastructure Security and Energy Restoration - Global Initiatives is currently working with several countries to improve critical energy infrastructure security by assessing their energy systems, identifying critical assets, and preparing and implementing energy infrastructure security plans."

Source: 2010 Energy Sector Annual Report

"The new Electric Sector Steering Group functions independently under its own charter for the purpose of fostering and facilitating, 'the coordination of sector-wide, policy-related activities and initiatives designed to improve the reliability and resilience of the electric sector, including physical and cyber security infrastructure.'"

Source: 2010 Energy Sector Annual Report

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

FOOD AND AGRICULTURE SECTOR

Partnership

The Food and Agriculture Sector is composed of complex production, processing, and delivery systems that encompass more than 2 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 Federal, State, tribal, territorial, and local representatives from agricultural, public health, food, law enforcement, and other relevant government entities. Sector Specific Agency (SSA) responsibility is shared between the U.S. Food and Drug Administration (FDA) and the U.S. Department of Agriculture (USDA).

Vision

The Food and Agriculture Sector acknowledges the Nation's critical reliance on food and agriculture. The sector will strive 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 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 the detection of a wide spectrum of threats
- Improve sector situational awareness through enhanced intelligence communication and information sharing
- Tailor risk-based, performance-based protection measures to the sector's physical and cyber assets, personnel, and customer products
- Address response and recovery at the sector level, not just as separate enterprises
- Expand laboratory systems and qualified personnel

Selected Accomplishments

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

- Released *Foreign Animal Disease Preparedness and Response Plan* and committed funding to the United Nations Food and Agriculture Organization to launch a crisis management center through the Highly Pathogenic Avian Influenza prevention and surveillance program
- Conducted three pilot tabletop exercises through The National School Lunch Program and will use feedback to finalize a resource kit for release in 2011
- Distributed more than 250,000 products related to the Employees FIRST Food Defense Awareness Training Kit and more than 3 million materials related to the Assure, Look, Employees, Report, Threat initiative
- Updated and validated three vulnerability assessments and completed two new assessments, including domestic and international transportation, through the USDA and the Food Safety and Inspection Service
- Updated and validated 12 vulnerability assessments and conducted four new vulnerability assessments, including baked goods and ice cream, through the FDA's Center for Food Safety and Applied Nutrition
- Added six member laboratories to the Food Emergency Response Network (FERN)
- Administered five proficiency tests for microbiological and chemistry target analysis through the FERN Proficiency Testing (PT) program, which included 226 participants from May 2009 to April 2010
- Conducted three exercises by the FERN Level 3 Biosafety Laboratory Triage Workgroup, which included a total of 425 individual analyses for five target organisms
- Participated in surveillance programs for Classical Swine Fever, bovine spongiform encephalopathy, chronic wasting disease and scrapie, swine influenza virus, and wild bird avian influenza through National Animal Health Laboratory Network laboratories
- Initiated a pseudo-rabies surveillance pilot project through the collaborative efforts of eleven laboratories and the USDA Animal and Plant Health Inspection Service

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
- Multi-State Partnership for Agriculture Security
- National Assembly of State Animal Health Officials
- National Association of County and City Health Officials
- National Association of State Departments of Agriculture
- National Center for Foreign Animal and Zoonotic Disease Defense
- National Environmental Health Association
- National Oceanic and Atmospheric Agency
- National Plant Board
- National Science Foundation
- The Navajo Nation
- Southern Agriculture and Animal Disaster Response Alliance
- State, Local, Tribal, and Territorial Government Coordinating Council
- U.S. Department of Agriculture
- U.S. Department of Commerce
- U.S. Department of Defense
- U.S. Department of Health and Human Services
- U.S. Department of Homeland Security
- U.S. Department of the Interior
- U.S. Department of Justice
- U.S. Environmental Protection Agency
- U.S. Food and Drug Administration

SCC MEMBERS

- American Bakers Association
- American Farm Bureau Federation
- American Frozen Food Institute
- American Feed Industry Association
- American Meat Institute
- American Veterinary Medical Association
- Archer Daniels Midland Company
- Association of Food Industries
- Cargill, Inc.

- Expanded certification for Phytophthora ramorum and citrus greening testing, executed two PT programs, and evaluated PT panels for two high-consequence regulatory plant pathogens through the National Plant Protection Laboratory Accreditation Program

Key Initiatives

The sector has a number of important initiatives underway 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 multiple pre-harvest and post-harvest surveillance programs
- 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 Initiative and the Post-harvest (Food) Research and Development for Biological and Chemical Agents Initiative
- Conducting vulnerability assessments for both pre-harvest and post-harvest (food)
- Maintaining strong laboratory networks
- Developing countermeasures for a food contamination or an animal health event
- Implementing recovery assistance development programs
- Developing information-sharing protocols and procedures and 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 protecting and enhancing the resilience of its critical infrastructure, including the following:

- Increase sector membership and encourage more active participation from current members
- Create a more effective and efficient information-sharing environment within the sector by leveraging and enhancing the Homeland Security Information Network (HSIN) and FoodSHIELD
- Create a three-year exercise schedule, planning for one large, multiagency exercise per year
- Continue to work on developing and raising sector partners' awareness of information sharing tools (e.g., HSIN, FoodSHIELD) and assessment tools (e.g., Food and Agriculture Sector Criticality Assessment Tool)

"FoodSHIELD currently has 2,312 registered users, and averages more than 16,000 hits per month."

Source: 2010 Food and Agriculture Sector Annual Report

"The first joint meeting between two U.S. regional agriculture alliances was held November 1–4, 2009, in Raleigh, NC. It was hosted by Multi-State Partnership for Security in Agriculture and North Carolina Department of Agriculture and Consumer Services."

Source: 2010 Food and Agriculture Sector Annual Report

"All manufacturing facilities producing foods for use in the national School Lunch Plan and warehouses storing these products prior to shipment for State-designated distribution centers have undergone a food defense audit conducted by the USDA Agriculture Marketing Service (USDA/AMS)."

Source: 2010 Food and Agriculture Sector Annual Report

- CF Industries, Inc.
- Chocolate Manufacturers Association
- ConAgra
- Consumer Specialty Products Association
- Council for Responsible Nutrition
- Dairy Institute of California
- Dean Foods Company
- Food Marketing Institute
- General Mills, Inc.
- Grocery Manufacturers Association
- H.J. Heinz Company
- International Association of Refrigerated Warehouses
- International Bottled Water Association
- International Dairy Foods Association
- International Food Service Distributors Association
- International In-flight Food Service Association
- International Warehouse Logistics Association
- Juice Products Association
- Kellogg Company
- Kraft Foods Global, Inc.
- McCormick & Company, Inc.
- Milkco, Inc.
- National Association of Convenience Stores
- National Cattlemen's Beef Association
- National Chicken Council
- National Corn Growers Association
- National Cotton Council of America
- National Fisheries Institute
- National Food Service Security Council
- National Grain and Feed Association
- National Milk Producers Federation
- National Oilseed Processors Association
- National Pork Board
- National Pork Producers Association
- National Renderers Association
- National Restaurant Association
- National Retail Federation
- North American Millers' Association
- PepsiCo, Inc.
- Publix
- Quaker Oats
- Snack Food Association
- Super Store Industry/ Turlock Dairy Division
- The Coca-Cola Company
- The Sugar Association
- Tyson Foods, Inc.
- United Fresh Produce Association
- USA Rice Federation
- U.S. Tuna Foundation

GOVERNMENT FACILITIES SECTOR

Partnership

The Government Facilities Sector (GFS) includes a wide variety of facilities owned or leased by Federal, State, local, tribal, or territorial governments, located both domestically and overseas. Although some types of government facilities are exclusive to the GFS, government facilities also exist in most other sectors. Many government facilities are open to the public for business activities, commercial transactions, provision of services, or recreational activities. Other facilities not open to the public contain highly sensitive information, materials, processes, and equipment. In addition to the facilities themselves, GFS considers elements associated with and often contained, or housed, within a facility. Under the National Infrastructure Protection Plan (NIPP), the Federal Protective Service (FPS) is assigned as the Sector-Specific Agency (SSA) responsible for the GFS.

The GFS also includes the Education Facilities Subsector, which consists of all schools, prekindergarten through 12th grade, public and private, and higher education, public and private, including proprietary schools, U.S. Department of Defense schools, and overseas schools assisted by the U.S. Department of State. This subsector includes both government-owned facilities and facilities owned by private-sector entities, so it faces some unique challenges.

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 partners work together to achieve the following sector-specific goals:

- Implement a long-term government facility risk management program
- Organize and partner for government facility protection and resilience
- Integrate government facility protection as part of the homeland security mission
- Manage and develop the capabilities of the GFS
- Maximize the 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:

- Increased the focus on cybersecurity across the sector
- Continued the commitment to research and development
- Reviewed and updated key risk-mitigation activities
- Strengthened sector coordination and partnerships to promote information sharing
- FPS rolled out the Risk Assessment and Management Program (RAMP)

Key Initiatives

FPS and partners are already implementing numerous protective programs that meet GFS goals and are contributing to a more secure sector. These protective programs range from visual situational awareness at major public events to Federal Emergency Management Agency continuity of operations. Key initiatives within the sector include the following:

- Conducting periodic building security assessments according to a schedule based upon each building's facility security level
- Promoting the awareness and implementation of Interagency Security Committee policies, guidelines, and best practices
- Maintaining and revising Occupant Emergency Plans that can reduce the threat to personnel, property, and other assets while minimizing work disruption
- Conducting thorough, efficient background investigations on contract guards by performing suitability reviews and background analysis using the Office of Personnel Management Electronic Questionnaires for Investigations Processing
- 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

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
- 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 the Interior
- U.S. Department of Justice

- 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
- Maintaining effective preventive and protective measures and programs through establishing best practices at MegaCenters

Path Forward

Numerous steps will be taken as GFS addresses challenges to its success, including the following:

- Enhance information technology (IT) systems and related operations to include systems and technologies for MegaCenters, RAMP, and other IT infrastructure, including database integration
- Continue to manage communications with internal and external security partners, and implement design and change management strategies to ensure that security partners are aware of and embrace changes in the FPS mission, organization, and processes consistent with the GFS Sector-Specific Plan
- Expand the available metrics to measure progress toward achieving GFS goals

Highlights of the 2010 Education Facilities Subsector Annual Report

Highlight 1: Creation of new training series online: "School Emergency Management."

Highlight 2: Published ED/USSS/FBI study on targeted violence at institutions of higher education.

Highlight 3: Creation of the School Dismissal Monitoring System.

"On April 12, 2010, the Interagency Security Council released the *Physical Security Criteria for Federal Facilities* and the *Design-Basis Threat Report*, which include new interim standards and how to address physical security measures for all Federal facilities."

Source: 2010 Government Facilities Sector Annual Report

"The State Messaging and Archival Retrieval Toolset program is delivering a new set of communication tools to the Department of State that provides widely needed all-hazards and cyber-threats critical infrastructure protection efforts."

Source: 2010 Government Facilities Sector Annual Report

"Completed 2,400 building security assessments prior to the deployment of the Risk Assessment and Management Program."

Source: 2010 Government Facilities Sector Annual Report

- U.S. Department of Labor
- U.S. Department of State
- U.S. Department of 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 compose 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 form 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 resilience 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 resilience of the HPH Sector, partners work together to achieve the following long-term, sector-specific 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 resilience of the HPH Sector. Some of the sector's accomplishments over the past year include the following:

- Increased participation in the support of medical supply chains during emergencies, through RxResponse, from 21 States in 2008 to all 50 States by the end of 2009
- Increased—by 20 percent—the number of metropolitan statistical areas that meet Cities Readiness Initiative criteria for effectively distributing medical countermeasures
- Developed and implemented an alerts-and-warnings process and supporting infrastructure to ensure the availability of timely and urgent information to sector partners in the event of an incident
- Expanded the Homeland Security Information Network Healthcare and Public Health portal user base to over 1,000 users and established the Information-Sharing Working Group
- Implemented the Private Sector Liaison Officer program
- Established a Cyber Security Work Group and began developing a sector-wide cybersecurity strategy

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 the Interior
- U.S. Department of Labor
- U.S. Department of Veterans Affairs

SCC MEMBERS

- Abbott Global Engineering Services
- AdvaMed
- Aetna, Inc.
- American Academy of Nurse Practitioners
- American Academy of Pediatrics
- American Academy of Physician Assistants
- American Association of Blood Banks
- American Association of Occupational Health Nurses
- American Association of Tissue Banks
- American College of Emergency Physicians
- American College of Occupational and Environmental Medicine
- American College of Physicians
- American Health Care Association
- American Hospital Association
- American Industrial Hygiene Association
- American Medical Association
- American Medical Depot
- American Nurses Association
- American Osteopathic Association
- American Red Cross
- American Society of Health System Pharmacists
- America's Health Insurance Plans
- Amgen, Inc.
- Association for Healthcare Resource and Materials Management
- Baxter Healthcare
- Biotechnology Industry Organization
- Blood Centers of America
- Blue Cross Blue Shield Florida
- Blue Shield California
- Blu-Med Response Systems
- Brooklawn Memorial Park
- Business Continuity Consulting
- Cardinal Health
- Casket and Funeral Supply Association of America
- Catholic Cemeteries, Diocese of Wilmington
- Catholic Cemetery Conference
- Cremation Association of North America
- Dartmouth Hitchcock Medical Center
- Dodge Company

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, and Project Public Health Ready
- Enhancing workforce protection through CDC's disease detection and investigation activities, the Strategic National Stockpile, and Cities Readiness Initiative
- Protecting physical assets through the CDC Select Agent Program and the Program Protection Office of the HHS Biomedical Advanced Research and Development Authority
- Mitigating risks associated with cybersecurity threats through efforts to develop a cybersecurity strategic plan

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:

- Expand information-sharing activities to include more original analysis and development of sector-specific risk products
- Integrate supply chain challenges more fully into overall sector risk analysis
- Apply a new comprehensive risk assessment methodology for sector asset prioritization

"When the 2009 H1N1 influenza emerged, the potential for viral transmission within healthcare facilities highlighted the need to keep healthcare workers safe."

Source: 2010 Healthcare and Public Health Sector Annual Report

"The rapid expansion of health information technology and the high reliance on these systems for sensitive health and claims data make the sector increasingly vulnerable to the consequences of cyber incidents."

Source: 2010 Healthcare and Public Health Sector Annual Report

"The sector established a Cyber Security Work Group (CSWG) that was tasked with developing a sector-wide cybersecurity strategy. The CSWG was successful in creating a framework that categorizes cyber risks and that can be used to examine areas where improved security would reduce an organization's vulnerability to cyber threats."

Source: 2010 Healthcare and Public Health Sector Annual Report

- Generic Pharmaceutical Association
- Genzyme Corporation
- George Washington University Medical Center
- Greater New York Hospital Association
- Group Health Cooperative
- Gunderson Lutheran Health Plan
- Hanover Hospital
- Health Industry Distributors Association
- Healthcare Distribution Management Association
- Healthcare Information and Management Systems Society
- Henry Schein, Inc.
- Hospital Association of Southern California
- Humana
- International Association for Healthcare Security and Safety
- International Cemetery, Cremation and Funeral Association
- James B. Haggin Memorial Hospital
- Johns Hopkins University
- Joint Commission on Accreditation of Healthcare Organizations
- Kaiser Permanente
- LabCorp
- Lafayette General Medical Center
- Matthews Cremation
- Medco Health Solutions
- Medline Industries
- Memorial Sloan Kettering Cancer Center
- MVP Health Care
- National Association of Chain Drug Stores
- National Association of Nuclear Pharmacies
- National Association of Psychiatric Health Systems
- National Council of State Boards of Nursing
- National Funeral Directors and Morticians Association
- Nevada Hospital Association
- Operation PAR
- Owens & Minor
- Pharmaceutical Research and Manufacturers of America
- Regence Group
- Regional Medical Center
- Samaritan Health Services
- Hunter College School of Nursing
- Siemens Healthcare USA
- Terumo Medical Corporation
- Texas A&M University
- Tuomey Healthcare System
- Universal Hospital Services
- University of Montana
- University of Pittsburgh Medical Center
- Walt Disney Company
- Washington Occupational Health Associates
- WellPoint
- Westchester Medical Association

INFORMATION TECHNOLOGY SECTOR

Partnership

The Critical Information Technology (IT) Sector produces and provides high-assurance IT products and services for all critical infrastructure sectors, private citizens, and commercial businesses. Collaboration among public and private sector partners is critical to ensure the protection and resilience of IT Sector functions upon which the sector and Nation depend. Private sector partners form 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 IT Sector also provides leadership to the Cross-Sector Cyber Security Working Group's (CSCSWG) cybersecurity mission by prioritizing topics for discussion and supporting targeted cybersecurity activities within the CSCSWG.

Vision

The IT Sector provides an infrastructure upon which all other critical infrastructure sectors rely. As such, the IT Sector's vision is to achieve a sustained reduction in the impact of incidents on the sector's critical functions. This vision supports the following:

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

Goals

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

- ***Prevention and Protection through Risk Management***—identify, assess, and manage risks to the IT Sector's critical functions and international dependencies
- ***Enhance Situational Awareness for Stakeholders at all Appropriate Levels***—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 or failures, or presidentially declared disasters
- ***Response, Recovery, and Reconstitution***—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 or failures, or presidentially declared disasters, and develop mechanisms for reconstitution
- ***Continuous Improvement***—drive continuous improvement of the IT Sector's risk management, situational awareness, and response, recovery, and reconstitution capabilities

Selected Accomplishments

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

- Completed a baseline IT Sector Risk Assessment in August 2009, which identified risks of concern and examples of existing and potential mitigations
- Developed an approach to sector risk management that enables sector partners to prioritize risks of concern and develop specific risk mitigation activities and associated metrics in order to address each risk of concern and track risk mitigation progress
- Commenced implementation of the risk management approach and identification of specific risk mitigation activities and metrics
- Advanced operational coordination among government and industry security partners, including IT Information Sharing and Analysis Center collocation with the DHS National Cybersecurity and Communications Integration Center

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

GCC MEMBERS

- National Association of State Chief Information Officers
- Office of the Director of National Intelligence
- State, Local, Tribal, and Territorial Government Coordinating Council
- U.S. Department of Commerce
- 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 the Interior
- U.S. Department of Justice
- U.S. Department of State
- U.S. Department of the Treasury
- U.S. Environmental Protection Agency

SCC MEMBERS

- AC Technology, Inc.
- Afilias USA, Inc.
- Anakam, Inc.
- Arxan Defense Systems, Inc. & Dunrath Capital
- BAE Systems
- Bearing Point
- Bell Security Solutions Inc.
- Bivio Networks
- Business Software Alliance
- CA Technologies
- Center for Internet Security
- Certichron, Inc.
- Cisco Systems, Inc.
- Computer and Communications Industry Association
- Computer Sciences Corporation
- Core Security Technologies
- Cyber Pack Ventures, Inc.
- Computing Technology Industry Association
- Concert Technologies
- Dell
- Deloitte & Touche LLP
- Dynetics
- Ebay
- Echelon One
- EDS
- EMC Corporation
- Entrust, Inc.
- EWA Information & Infrastructure Technologies, Inc.
- General Dynamics
- Green Hills Software
- Google
- Hatha Systems

- Building on the sector baseline risk assessment to assess and manage cross-sector risks and interdependencies and to refine metrics and protective programs
- Coordinating across critical infrastructure sectors on response and recovery activities through the IT Information Sharing and Analysis Center 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
- Providing leadership for cross-sector cybersecurity through the CSCSWG and other information sharing and protective security programs, including the US-CERT
- Providing proper and consistent security training, at both the national and organizational levels, to educate about the importance and impact of cybersecurity
- Employing numerous security practices to mitigate supply-chain risks

Path Forward

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

- Evaluate the risks to the *Provide Identity Management and Associated Trust Support Services* critical IT Sector function, and the risks to the IT Sector associated with a dependency on the Communications and Energy Sectors
- Ensure continued coordination and cohesion between industry and government in prioritizing and mitigating the risks identified in the baseline IT Sector Risk Assessment
- Continue to work with DHS Infrastructure Protection and other partners to increase awareness and understanding of the sector's function-based risk management approach and demonstrate how risk can be addressed through implementation of the top-down approach
- Ensure coordination between industry and government to identify and prioritize IT Sector strategic risk considerations
- Continue to work with the cross-sector community to increase awareness of cybersecurity risks and dependencies, and support targeted cybersecurity activities

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

"The IT Sector participated in a number of key DHS and White House initiatives during the 2009–2010 NIPP reporting cycle, including the National Cyber Incident Response Plan, the National Strategy for Secure Online Transactions, the DHS Global Supply Chain Risk Management program, and National Level Exercise 2010 and Cyber Storm III planning."

Source: 2009 Information Technology Sector Annual Report

"The IT Sector has distinct [critical infrastructure] protection responsibilities because it includes virtual and distributed infrastructure that support critical IT Sector functions that all other [critical infrastructure] rely on for effective and secure operations."

Source: 2009 Information Technology Sector Annual Report

- IBM Corporation
- Information Systems Security Association
- Intel Corporation
- Information Technology Industry Council
- Information Technology - Information Sharing & Analysis Center
- International Systems Security Engineering Association
- Internet Security Alliance
- IBM Internet Security Systems, Inc.
- International Security Trust and Privacy Alliance
- ITT Corporation
- Juniper Networks
- KPMG LLP
- L-3 Communications
- Lancope, Inc.
- Litmus Logic
- LGS Innovations
- Lockheed Martin
- Lumeta Corporation
- Lunar Line
- McAfee, Inc.
- Microsoft Corporation
- NetStar-1
- Neustar
- Northrop Grumman
- NTT America
- One Enterprise Consulting Group, LLC
- Raytheon
- Reclamere
- Renesys Corporation
- Research in Motion
- SAFE-BioPharma Association
- SafeNet Government Solutions
- Seagate Technology
- Secure Computing
- SecureState
- Sentar Inc.
- Serco International
- Siemens Healthcare
- SI International
- Sun Microsystems, Inc.
- Symantec Corporation
- System 1
- Team Cymru
- TechAmerica
- Telecontinuity, Inc.
- Terremark
- TestPros, Inc.
- Triumfant
- U.S. Internet Service Provider Association
- Unisys Corporation
- 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 monuments or icons (e.g., Golden Gate Bridge, Hoover Dam, and the U.S. Capitol), other partners have responsibility for protection of these types of facilities. The NMI Sector partnership consists of only Federal entities, though it has partnered with the Government Facilities Sector to coordinate outreach to the various State, local, and tribal entities. The U.S. Department of the Interior (DOI) serves as the Sector-Specific Agency for the NMI Sector. DOI is responsible for approximately 1.3 million visitors daily, and more than 507 million acres of public land, including 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 an 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, partners work together to achieve the following sector-specific security goals:

- Continue to review sector criteria to ensure a clear definition of NMI Sector assets
- Delineate and define roles and responsibilities for sector 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 operate sector assets
- Maintain seamless coordination among GCC partners that operate sector assets
- Maintain cross-sector coordination with regard to NMI Sector assets whose primary protective responsibility resides in another sector
- Integrate robust security, technology, and practices contingent on agency mission priorities and available resources while preserving the appearance and accessibility of 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 resilience of the NMI Sector. Some of the sector's accomplishments over the past year include the following:

- Conducted training exercises through the U.S. Park Police Special Weapons and Tactics team and the Marine Patrol in New York
- Increased physical security awareness through multiple Protective System Assessments conducted by DHS
- Enhanced the Smithsonian Institution security
- Implemented the protection of network systems
- Established the Icon Security Council through the efforts of the National Park Service to provide a greater means of sharing Law Enforcement significant incident information
- Established a partnership between the Independence Hall Historic Park and the Philadelphia Police Department

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
  - U.S. Secret Service
- U.S. Department of the Interior
  - National Park Service
  - Office of Law Enforcement, Security, and Emergency Management
  - U.S. Park Police
- U.S. Department of Justice
  - Federal Bureau of Investigation

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 biannual (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 the following:

- Completing blast assessments at all NMI assets
- Implementing civil aviation restrictions around critical infrastructure assets located outside the Washington, D.C. metropolitan area
- Researching, developing and identifying new technologies to maintain a controlled perimeter and to provide accessibility through new techniques for visitor screening and surveillance
- Implementing Stationed Radar Sensors that can detect either moving or stationary targets
- Promoting the use of the Homeland Security Information Network 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
- Assess new avenues for the provision of resources in an effort to protect the public at NMI assets
- Conduct additional research into the nature, extent, and duration of cognitive impacts from terrorist attacks, such as the "rally effect"
- Continue to encourage sector partners to perform or update protective systems assessments at NMI Sector assets
- Continue to promote and facilitate intelligence and information sharing, effective security practices, Science and Technology Directorate critical infrastructure initiatives, and training opportunities among the GCC partners
- Encourage sector partners to work with local law enforcement and emergency responders with resources to enhance security "outside the fence" utilizing the Buffer Zone Protection Program

"The National Monuments and Icons (NMI) Sector Government Coordinating Council provides an effective mechanism for coordinating [critical infrastructure] strategies and activities, policy, and communication across the government and between the government and the NMI Sector to support the Nation's homeland security mission."

Source: 2010 National Monuments and Icons Sector Annual Report

"The Smithsonian Institution Anti-Terrorism Program is designed to protect the staff, visitors, national collections, and facilities entrusted to the care of the Institution from an all-hazard incident. The intent of the program is to measure risks to the Institutions to adequately mitigate risks."

Source: 2010 National Monuments and Icons Sector Annual Report

"The National Monuments and Icons Sector continues to successfully use the [Homeland Security Information Network – Critical Sectors] portal to enable sector partners to quickly share information concerning all-hazard threats and protective measures. Recently, DOI SSA worked with DHS to upgrade the portal to give sector partners a wider range of capabilities."

Source: 2010 National Monuments and Icons Sector Annual Report

NUCLEAR SECTOR

Partnership

The Nuclear Sector includes the Nation's 65 commercial nuclear power plants, which provide nearly 20 percent of the U.S. electricity generation capacity. 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 three subcouncils, in addition to special working groups, to address protection and resilience efforts specific to research and test reactors, radioisotopes, and cybersecurity. The U.S. Department of Homeland Security Office of Infrastructure Protection serves as the Sector-Specific Agency 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 protection and resilience of the Nuclear Sector in an all-hazards environment; and to lead by example to improve the Nation's overall critical infrastructure readiness.

Goals

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

- Establish permanent and robust collaboration and communication among sector partners that have security and emergency responsibilities for the Nuclear Sector
- Obtain cross-sector dependency and interdependency-related information and share with sector partners
- Increase public awareness of sector protective measures, consequences, and proper actions following the 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 sector partners to develop measures and procedures to prevent, protect, respond, and recover from all-hazard disasters impacting Nuclear Sector assets
- Protect against the exploitation of the Nuclear Sector's cyber assets, systems, and networks, and the functions they support
- Use a risk-informed approach that includes protection and resilience considerations to make budgeting, funding, and grant decisions on potential protection and emergency response enhancements

Selected Accomplishments

Sector partners continue to maintain and enhance the safety, security, and resilience of the Nuclear Sector. Accomplishments over the past year include the following:

- Continued implementation of Nuclear Regulatory Commission (NRC) regulatory programs based on a single set of principles and philosophies to ensure plant and radiological safety, security, and emergency preparedness at operating nuclear power plants
- Completed second Integrated Pilot Comprehensive Exercise at the Donald C. Cook Nuclear Power Plant
- Implemented a new NRC cybersecurity requirement stating nuclear power plant owners and operators must provide high assurance that key digital information systems and networks, such as those associated with safety, security, and emergency preparedness functions, are adequately protected against cyber attacks
- Recovered 4,358 disused radioactive sources in FY 2009, and more than 24,000 since 1997
- Retrofitted 167 irradiators with in-device delay kits designed to make the unauthorized removal of radioactive materials from high-risk irradiators more difficult, as of May 2010
- Implemented the National Source Tracking System, through the NRC, providing administrative accountability for more than 70,000 high-risk radioactive sources

Key Initiatives

The Nuclear Sector and its partners are implementing numerous protective programs and initiatives to help sustain the high-security posture of sector assets while addressing emerging risks.

Key initiatives within the sector include the following:

- Implementing additional voluntary security enhancements such as the Research and Test Reactors Voluntary Security Enhancement Project, Radiological Site Voluntary Security Enhancement Project, and Cesium Chloride Irradiator In-Device Delay Program
- Conducting Integrated Pilot Comprehensive Exercises, biennial emergency preparedness exercises, and emergency preparedness drills using hostile action-based scenarios as initiating events

GCC MEMBERS

- Nuclear Regulatory Commission
- State of Delaware
- State of Florida, Department of Health
- Commonwealth of Massachusetts, Department of Public Health
- Commonwealth 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
  - Federal Bureau of Investigation
- U.S. Department of State
- U.S. Department of Transportation
- U.S. Environmental Protection Agency

- Facilitating responses to security threats at facilities with nuclear or radiological materials through the Alarm Responder Training Program and tabletop exercises
- Assessing the adequacy of State, local, and tribal government emergency plans through the Radiological Emergency Preparedness Program
- Conducting force-on-force security inspections to assess nuclear plants' ability to defend against the Design Basis Threat
- Conducting FBI outreach visits to select facilities housing risk-significant radioactive materials
- Recovering excess, unwanted, abandoned, or orphaned radioactive sealed sources

Path Forward

The Nuclear Sector still faces some critical infrastructure protection and resilience challenges, such as enhancing integrated response capabilities, ensuring the security of cyber-based systems, ensuring safe and secure storage or disposal for commercial sealed sources, and increasing the resilience of the radioisotopes supply chain. The sector will take the following steps to address these challenges:

- Continue to coordinate with State and local authorities and with the private sector, as appropriate, to promote adequate, consistent, and integrated response preparedness and coordination across the sector
- Continue to identify cybersecurity risks that could potentially affect the Nuclear Sector and determine mitigation strategies through development of the *Roadmap for Enhancing Industrial Control Systems Security* in the Nuclear Sector, modeled upon roadmaps created for the Chemical, Energy, and Water Sectors
- Remain cognizant of efforts taken pursuant to recommendations of the Removal and Disposition of Disused Sources (RDDS) focus group, which developed a single, clear message on potential national security concerns presented by the lack of commercial disposal options for sealed sources
- Support radioisotopes supply-chain resilience by participating in interagency efforts to explore options to enhance supplies of key radioisotopes, such as Molybdenum-99

"In December 2009, the joint public and private-sector working group referred to as the Comprehensive Review Outcomes Working Network was formally concluded. CROWN had successfully tracked the implementation of hundreds of security and preparedness enhancements identified during the Comprehensive Reviews at nuclear power plants by State and local emergency-management and law-enforcement organizations responsible for responding to an event at those plants. These enhancements are voluntary and seek to improve security and preparedness beyond what is required by regulation."

Source: 2010 Nuclear Sector Annual Report

"The Nuclear Sector remains among the most secure of the 18 [critical infrastructure] sectors, and Nuclear Sector partners seek to maintain and improve the sector's security posture in light of a changing risk landscape ... Regulatory developments include implementation of a new requirement that nuclear power plant owners/operators must provide high assurance that key digital information systems and networks, such as those associated with safety, security, and emergency preparedness functions, are adequately protected against cyber attacks. Voluntary developments include further progress in the Department of Energy National Nuclear Security Agency's projects to make the radiological materials used in the sector more secure. "

Source: 2010 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
- Exelon Generation Company, LLC
- Florida Power and Light
- General Electric
- National Institute of Standards and Technology
- Nuclear Energy Institute
- Oregon State University
- QSA Global
- Southern Nuclear Company
- University of Missouri
- 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. Government, businesses, and private citizens rely daily on the efficient and timely functioning of this sector. The P&S Sector is mainly composed of four large, integrated carriers that represent 94 percent of the sector: the United States Postal Service (USPS), the United Parcel Service (UPS), FedEx, and DHL International. The remainder of the sector consists of smaller firms providing regional and local courier services, other mail services, mail management for corporations, and chartered air delivery services. USPS, UPS, FedEx, and DHL make up the Sector Coordinating Council (SCC), while members from the key Federal agencies form the Government Coordinating Council (GCC). The Transportation Security Administration serves as the Sector-Specific Agency.

Vision

Ensure continuity of operations, ease of use, and public confidence in the P&S Sector by creating a multi-layered security posture that integrates public and private 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 P&S Sector, partners work together to achieve the following sector-specific goals:

- Create incident-reporting mechanisms and awareness/outreach programs with the law enforcement and intelligence communities to facilitate a better understanding of the information requirements of the P&S 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
- Implement risk-based security measures for transportation assets, processing and distribution centers, and information technology centers that are tailored to the size of implementing organizations and scalable to accommodate both routine protective requirements and periods of heightened alert
- Work to deny terrorists the ability to exploit or replicate the trusted access that sector personnel have to public and private facilities in collecting, transporting, and delivering 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 terrorist attacks, threats and disruptions, crippling attacks (cyber or physical), or other intentional or unintentional incidents; 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 nationally or regionally critical emergency and develop coordinated plans to ensure that such items can be delivered to affected areas quickly
- Facilitate close partnerships with other sectors as appropriate to enable rapid identification, decontamination, and treatment of incidents in the P&S Sector
- Develop national, regional, and local public communication protocols to inform U.S. citizens of incidents in the sector and minimize disruptions to their P&S transactions

Selected Accomplishments

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

- Prepared the *2010 Postal and Shipping Sector-Specific Plan*
- Prepared the *2010 Postal and Shipping Sector Annual Report*
- Identified sector risk-mitigation activities
- Participated in the DHS National Operations Center and the FBI National Joint Terrorism Task Force
- Maintained and updated the Homeland Security Information Network portal.
- Completed security assessment reviews of sector facilities
- Continued to collaborate with DHS on the Cities Readiness Initiative (CRI)
- Supported investigations of anthrax threats and suspicious letters

GCC MEMBERS

- Office of the Director of National Intelligence
- U.S. Department of Commerce
- U.S. Department of Defense
- U.S. Department of Health and Human Services
- U.S. Department of Homeland Security
- U.S. Department of Justice
- U.S. Department of State
- U.S. Department of Transportation
- U.S. Postal Service

Key Initiatives

The P&S Sector is implementing various programs to enhance the security and resilience of its assets. Key initiatives within the sector include the following:

- Targeting high-value cyber crimes
- Mitigating risks to new postal products and business planning
- 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 sector CRI
- Improving sector resilience
- Enhancing emergency preparedness
- Facilitating the sharing of security information

Path Forward

The P&S 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 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 sector-specific preparedness standards
- 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, resilience, 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 resilience 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

"The Postal and Shipping Sector is responsible for the reliable delivery of more than 177 billion letters and packages annually."

Source: 2010 Postal and Shipping Sector Annual Report

"Postal and Shipping Sector owners and operators responded to dozens of emergencies in Fiscal Year 2009 related to hurricanes, floods, fires, and other incidents."

Source: 2010 Postal and Shipping Sector Annual Report

"During Fiscal Year 2009, Postal Inspectors screened mail at 17 events, including the National Football League's Super Bowl XLIII and the G-20 Economic Summit in Pittsburgh, PA."

Source: 2010 Postal and Shipping Sector Annual Report

"Postal and Shipping Sector operations focused on three areas of concern in maintaining public confidence in the mail: global security, homeland security, and revenue fraud."

Source: 2010 Postal and Shipping Sector Annual Report

SCC MEMBERS

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

TRANSPORTATION SYSTEMS SECTOR

Partnership

The Transportation Systems Sector is a vast, open network of interdependent systems that move millions of passengers and millions of tons of goods annually. The Transportation Systems Sector partnership framework includes a Government Coordinating Council (GCC), a Sector Coordinating Council (SCC), and subsector GCCs and SCCs for each of the six transportation modes: Aviation, Maritime, Mass Transit, Highway, Freight Rail, and Pipeline. The GCC consists of members from key Federal, State, and local agencies. The sector level SCC – including leading associations, owners and operators, and other private sector entities with transportation security responsibilities – is being revamped to expand its coverage and representation. Currently, the subsector SCCs are the primary coordination venue for private sector collaboration within each transportation mode. The Transportation Security Administration serves as the Sector-Specific Agency (SSA) for the Transportation Systems Sector, and the U.S. Coast Guard serves as the Maritime Mode SSA. The Department of Transportation provides Federal leadership on the sector's preparedness for natural disasters, and in emergency response and recovery support functions.

Vision

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

Goals

The sector's mission is to continuously improve the security posture of transportation systems serving the Nation. This mission is guided by the following four goals:

- Prevent and deter acts of terrorism using, or against, the transportation system
- Enhance the all-hazards preparedness and resilience of the global transportation system to safeguard U.S. national interests
- Improve the effective use of resources for transportation security
- Improve sector situational awareness, understanding, and collaboration

Selected Accomplishments

The Transportation Systems Sector has made many improvements to the security posture of this sector. Some of these improvements include the following:

- Increased deployment of advanced screening, vetting, tracking, and communications technologies
- Completed comprehensive aviation and surface risk assessment comparing more than 300 risk scenarios to inform prioritization of modal risks
- Increased unannounced deployments of Visible Intermodal Prevention and Response teams to reduce risk of attacks in sensitive locations
- Extended risk-based grant programming opportunities to transportation entities with the highest risk of terrorist attacks
- Launched the freight rail Homeland Security Information Network, with the SSA nominating and validating 35 new users since its launch
- Achieved 100 percent screening of cargo on domestic passenger flights
- Conducted and supported 14 exercises and six other events, such as workshops, through the Intermodal Security Training Exercise Program (I-STEP)
- Continued to implement advanced screening technologies to prevent and deter acts of terrorism in the aviation mode
- Completed the National Transportation System Recovery Plan
- Conducted more than 200 foreign port assessments in 70 countries through the International Ship and Port Facility Security Program

Key Initiatives

The Transportation Systems Sector is undertaking a wide variety of initiatives to enhance protection and resilience. Several of these initiatives involve the modal GCCs bringing together numerous government agencies to collaborate on security efforts ranging from creating a highway-sensitive-materials tracking program, to improving information-sharing methods among sector partners. Key initiatives within the sector include the following:

- Screening and vetting of transportation workers through the Transportation Worker Identification Credential initiative and the Hazardous Materials Endorsement Threat Assessment Program
- Securing critical physical infrastructure through the national tunnel security initiative, general aviation airport security measurements, and Area Maritime Security Plans
- Reducing freight rail risks using Global Positioning System technology on Toxic Inhalation Hazard cargo shipments
- Leveraging technologies to screen workers, travelers, and cargo through the Secure Flight and Checkpoint Evolution programs

GCC MEMBERS

- American Association of State Highway and Transportation Officials
- Federal Energy Regulatory Commission
- Nuclear Regulatory Commission
- Transportation Security Administration
- U.S. Coast Guard
- 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 the Interior
- U.S. Department of Justice
- U.S. Department of State
- U.S. Department of Transportation
- U.S. Department of the Treasury

- Conducting security awareness and response training programs such as the Federal Flight Deck Officers and Flight Crew Member Self-Defense Training programs
- Increasing risk awareness in decisionmaking processes through refinement and expansion of risk methodologies, such as the Bridge Criticality Tool, the Maritime Security Risk Analysis Model, and the Transportation Sector Security Risk Assessment
- Evaluating the vulnerability of critical transportation infrastructure through the Baseline Assessment for Security Enhancement and general aviation airport security measurement programs
- Developing a comprehensive strategic approach for identifying and managing cybersecurity risks to critical infrastructure operations

Path Forward

The Transportation Systems Sector is moving forward through regulatory and voluntary risk management initiatives to secure its critical infrastructure and resources. Some of these steps include the following:

- Apply the National Infrastructure Protection Plan and sector risk management framework consistently across modes
- Continue to work with the intelligence community to optimize the timely and effective flow of intelligence information to stakeholders
- Conduct periodic sector-wide risk assessments
- Issue regulations for security plans, assessments, and training for those elements of the surface modes identified in the 9/11 Act
- Work within the critical infrastructure partnership model and with cybersecurity professionals to develop strategies to protect and defend against, respond to, and recover from attacks on critical cyber systems

Transportation Systems Sector

Government Coordinating Council	Sector Coordinating Council
Aviation Mode GCC	Aviation Mode SCC
Mass Transit Mode GCC	Mass Transit Mode SCC
Freight Rail Mode GCC	Freight Rail Mode SCC
Maritime Mode GCC	Maritime Mode SCC
Highway Mode GCC	Highway Mode SCC
Pipelines Mode GCC	Pipelines Mode SCC

SCC members are represented at the modal level shown on the next page.

"The primary focus of the sector's risk management process ... was the identification, prioritization, and reduction of risks to transportation critical infrastructure..."

Source: 2010 Transportation Systems Sector Annual Report

"Sector partners continue to leverage various new and emerging technologies, such as screening and communications technologies, as critical components of the sector's flexible, layered security strategy."

Source: 2010 Transportation Systems Sector Annual Report

"The Quadrilateral Agreement among Australia, Canada, [the European Union], and the United States has the goal of ensuring equivalent overall levels of air cargo security among partners."

Source: 2010 Transportation Systems Sector Annual Report

"To further reduce risk and deter acts of terrorism, the sector has implemented programs that add a layer of unpredictability to existing security measures."

Source: 2010 Transportation Systems Sector Annual Report

TRANSPORTATION SYSTEMS SECTOR

AVIATION MODE SCC MEMBERS

- Aerospace Industries Association
- Air Carrier Association of America
- Air Transport Association
- Aircraft Owners and Pilots Association
- Airport Consultants Council
- Airports Council International - North America
- American Association of Airport Executives
- The Boeing Company
- Cargo Airline Association
- National Air Carrier Association
- National Air Transportation Association
- National Business Aviation Association, Inc.
- Regional Airline Association

HIGHWAY AND MOTOR CARRIER MODE SCC MEMBERS

- American Trucking Associations
- American Bus Association
- American Chemistry Council
- American Petroleum Institute
- Border Trade Alliance
- The BusBank
- Con-Way, Inc.
- Detroit-Windsor Truck Ferry
- First Student
- Institute of Makers of Explosives
- Intelligent Transportation Society of America
- Intermodal Association of North America
- Kenan Advantage Group
- Mid-States Express, Inc.
- National Association of Small Trucking Companies
- National School Transportation Association
- National Tank Truck Carriers, Inc.
- Owner-Operator Independent Drivers Association
- PITT Ohio
- SLT Express
- Taxicab, Limousine and Paratransit Association
- Tri-State Motor Transit Company
- Truck Manufacturers Association
- Truck Rental and Leasing Association
- United Motorcoach Association

MARITIME MODE SCC MEMBERS

- American Association of Port Authorities
- American Waterways Operators
- Chamber of Shipping of America
- Donjon-Smit, LLC
- International Council of Cruise Lines
- National Maritime Safety Association
- National Waterways Conference
- Offshore Marine Service Association
- Passenger Vessel Association
- World Shipping Council

MASS TRANSIT MODE SCC MEMBERS

- American Public Transportation Association
- Berks Area Reading Transportation
- Capital Metro, Austin, TX
- Community Transportation Association of America
- Dallas Area Rapid Transit (DART)/ Trinity Railway Express
- Hampton Roads Transit
- Metrolink, Rock Island, IL
- Metropolitan Transportation Authority, State of New York
- New Jersey Transit Authority
- Port Authority Trans-Hudson
- San Francisco Municipal Transportation Agency
- Utah Transit Authority
- Washington Metropolitan Area Transit Authority

PIPELINE MODE SCC MEMBERS

- American Gas Association
- American Petroleum Institute
- Association of Oil Pipe Lines
- Colonial Pipeline
- Dominion Resources Inc.
- Enbridge
- Genesis Energy
- Interstate Natural Gas Association of America
- Kinder Morgan
- NiSource Inc.
- Questar
- Spectra Energy
- Williams

RAILROAD MODE SCC MEMBERS

- Association of American Railroads
- American Short Line and Regional Railroad Association
- Amtrak
- Anacostia and Pacific
- BNSF Railway Company
- Canadian National
- Canadian Pacific Railway
- CSX Transportation
- Genesee & Wyoming
- Iowa Interstate Railroad Ltd
- Kansas City Southern Railway Company
- Metra
- Norfolk Southern
- RailAmerica
- Union Pacific Railroad Company
- Wheeling & Lake Erie Railway

WATER SECTOR

Partnership

There are more than 153,000 public drinking water systems and approximately 16,500 wastewater treatment 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 has its sanitary sewage treated by these wastewater systems. Successful attacks on Water Sector assets could result in a large number of illnesses or casualties or a denial of service that 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 that 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

A secure and resilient drinking water and wastewater infrastructure that provides clean and safe water is an integral part of daily life—ensuring the economic vitality of and public confidence in the Nation's drinking water and wastewater services through a layered defense of effective preparedness and security practices in the sector.

Goals

Water Sector partners are collaborating to achieve the following sector 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:

- Supported a Water Security Initiative pilot in Cincinnati to successfully operate all five monitoring and surveillance components of its drinking water contamination warning systems
- Began four additional Water Security Initiative pilots to design and deploy drinking water contamination warning system equipment
- Developed the *Roadmap to a Secure & Resilient Water Sector and the Roadmap to Secure Control Systems in the Water Sector*, a unified security strategy containing specific goals, milestones, and activities to mitigate cybersecurity risk over the next 10 years
- Combined the 11 existing Regional Laboratory Response Plans into a single National Plan
- Published the *Water Sector Measures Analysis* report covering measures for utilities and "other actors" including States, Federal agencies, and Water Sector associations; currently developing the second annual performance metrics process
- Upgraded existing Water Sector risk assessment methodologies (e.g., Risk Assessment Methodology for Water Utilities, the Security and Emergency Management System, and Vulnerability Self-Assessment Tools (VSAT))
- Finalized VSAT, which allows drinking water and wastewater owners and operators to assess the risk of terrorism, hurricanes, tornadoes, floods, and earthquakes at their utilities
- Finalized the Water Health and Economic Analysis Tool, including drinking water modules for hazardous gas and loss of operating assets scenarios
- 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
- Increased efforts to promote the establishment of intrastate mutual aid and assistance agreements, such as the Water-Wastewater Agency Response Network (WARN)
- Developed tools and extensive training programs to help utilities enhance their emergency preparedness and communicate with local first responders and public health providers such as the Incident Command System and National Incident Management System

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
- New York City Department of Environmental Protection
- U.S. Army Corps of Engineers
- 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 the Interior
- U.S. Department of Justice
- U.S. Department of State
- U.S. Environmental Protection Agency

Key Initiatives

The Water Sector's protective programs and actions are interrelated and designed to strategically address the sector's security goals and associated objectives. These encompass the EPA's four 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 the following:

- Implementing the Water Security Initiative, which aims to detect and appropriately respond to drinking water contamination threats and incidents and publish guidance documents to assist utilities in designing, developing, and deploying contaminant detection and warning systems
- Enhancing the security of drinking water utilities through the development of the Water Laboratory Alliance laboratory network
- Developing an all-hazards, consequence-management planning document to evaluate preparedness, emergency response, and recovery priorities and identifying actions needed to implement these priorities through the use of a Critical Infrastructure Partnership Advisory Council (CIPAC) working group
- Evaluating progress made toward critical infrastructure protection and resilience
- Conducting and updating risk assessments
- Preparing and revising emergency response plans
- Developing and improving the 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 protection and resilience of its assets, including the following:

- Follow up on sector-specific metrics
- Continue sector strategic planning, cybersecurity, and decontamination efforts
- Coordinate research and development efforts
- Advance WARN use and business continuity planning
- Conduct dependency and interdependency training for water utilities across all 18 critical infrastructure sectors
- Enhance ongoing partnership efforts of the Water SCC, GCC, and CIPAC working groups

"The *Roadmap to Secure Control Systems in the Water Sector* establishes a strategy framework for a path forward in the near and midterm, to improve the security and resilience of the Water Sector."

Source: 2009 Water Sector Annual Report

"The Water Contaminant Information Tool is a comprehensive database of information for 102 chemical, biological, and radiological contaminants of concern to the Water Sector."

Source: 2009 Water Sector Annual Report

"WaterISAC [Water Information Sharing and Analysis Center] is a secure, Internet-based, rapid notification system and information resource for gathering, evaluating, conveying, and sharing security-related information on drinking water and wastewater systems; communications are geared to utility executives, managers, operators, and security officers (www.waterisac.org)."

Source: 2009 Water Sector Annual Report

SCC MEMBERS

- American Water
- American Water Works Association (AWWA)
- Artesian Water Company
- Association of Metropolitan Water Agencies
- Bean Blossom-Patricksburg Water Corporation
- Boston Water and Sewer Commission
- Breezy Hill Water and Sewer Company
- California Water Service, Co.
- City of Portland Bureau of Environmental Services
- King County Department of Natural Resources and Parks
- Lafayette Utilities System
- National Association of Clean Water Agencies
- National Association of Water Companies
- National Rural Water Association
- Onondaga County Water Authority
- Pima County Wastewater Management Department
- Prince William County Water Authority
- Trinity River Authority of Texas
- United Water
- Water Environment Federation
- Water Environment Research Foundation
- Water Research Foundation

Homeland
Security