2011 Critical Infrastructure Partnership Advisory Council ANNUAL

Homeland Security

2011 Critical Infrastructure Partnership Advisory Council
ANNUAL

CONTENTS

CRITICAL INFRASTRUCTURE PARTNERSHIPS 2

CROSS-SECTOR PARTNERSHIPS 6

- CIKR Cross Sector Council 6
- Federal Senior Leadership Council 8
- State, Local, Tribal, and Territorial Government Coordinating Council 10
- Regional Consortium Coordinating Council 12

SECTOR PARTNERSHIPS 14

- Banking and Finance Sector 14
- Chemical Sector 16
- Commercial Facilities Sector 18
- Communications Sector 20
- Critical Manufacturing Sector 22
- Dams Sector 24
- Defense Industrial Base Sector 26
- Emergency Services Sector 28
- Energy Sector 30
- Food and Agriculture Sector 32
- Government Facilities Sector 34
- Healthcare and Public Health Sector 36
- Information Technology Sector 38
- National Monuments and Icons Sector 40
- Nuclear Sector 42
- Postal and Shipping Sector 44
- Transportation Systems Sector 46
- Water Sector 50

CRITICAL INFRASTRUCTURE PARTNERSHIPS

Introduction

The protection and resilience of the Nation's critical infrastructure is a shared responsibility between all levels of government and critical infrastructure owners and operators. As such, public-private sector partnerships are central to success in this inherently complex mission. The National Infrastructure Protection Plan (NIPP) relies on a sector partnership model, illustrated in Figure 1, as the primary organizational structure for coordinating critical infrastructure activities across the 18 critical infrastructure sectors identified by Congress and within the NIPP.

The Critical Infrastructure Partnership Advisory Council (CIPAC) structure provides the legal framework for members of the Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs) to work together on critical infrastructure efforts, including:

- Planning, developing, and implementing protection and resilience programs
- Coordinating operational activities, including incident response and recovery
- Developing and supporting national policies and plans, including Sector-Specific Plans

The *2011 CIPAC Annual* describes the maturity of partnership collaboration over the past year for the four cross-sector councils and the 18 critical infrastructure sectors. It presents the composition, vision, goals, selected accomplishments, key initiatives, and path forward for each sector or cross-sector council partnership.

CIPAC members are institutions represented by including 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. The U.S. Department of Homeland Security (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, pursuant to section 871 of the Homeland Security Act. The CIPAC charter was subsequently renewed through the Federal Register Notices published on April 30, 2008 and April 22, 2010.

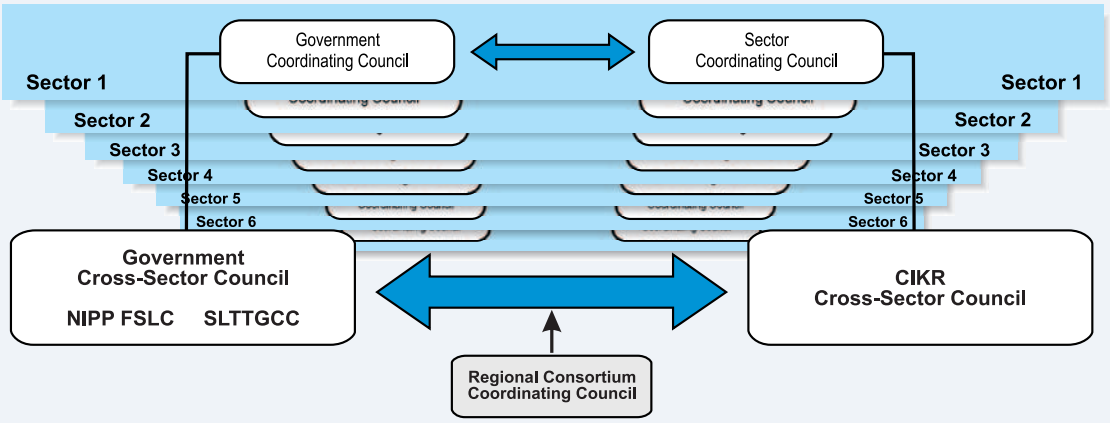
An SCC is the principal entity for owners and operators to coordinate with the government on critical infrastructure protection and resilience activities and issues. A GCC is the government counterpart for each SCC and facilitates interagency and cross-jurisdictional coordination. The 18 critical infrastructure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

Cross-Sector Councils

CIPAC cross-sector forums promote coordination, communication, and the sharing of effective practices across critical infrastructure sectors, jurisdictions, or specifically defined geographical areas. These forums include:

- The ***Critical Infrastructure and Key Resources (CIKR) Cross Sector Council*** addresses cross-sector issues and interdependencies among the SCCs, and consists of the leadership of each of the SCCs.
- The ***Government Cross Sector Council*** addresses interagency, 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).

Figure 1. National Infrastructure Protection Plan Sector Partnership Model



- 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 equivalent 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.

CIPAC Support and the Critical Infrastructure and Key Resources Information-Sharing Environment

The DHS National Protection and Programs Directorate's Office of Infrastructure Protection (NPPD/IP) is the national coordinator for the critical infrastructure protection mission. As a steward of the NIPP and its sector partnership, NPPD/IP offers secretariat and analytical support to the NIPP sector partnership councils. This support has enabled the number of CIPAC-related activities to continue to grow every year. Highlights of this growth include:

- CIPAC membership institutions have significantly increased in the last three years, from 643 member organizations in 2009 to 1,871 members in 2011.
- Councils and their working groups held more than 650 meetings in 2010, a 32 percent increase from 2009.

Central to NPPD/IP support of the sector partnership is its management of the CIKR Information Sharing Environment (ISE). As a unique capability, the CIKR ISE provides GCCs and SCCs with procedures, content, and tools that enable critical infrastructure mission partners to share the vital information that is needed to manage risk and respond to disruptions.

The *2011 CIPAC Annual* describes the extent to which the sector councils have built and sustained their information-sharing capabilities through the CIKR ISE. Overall, the past year saw a marked increase in the number of active users participating in the environment, increased availability and dissemination of actionable content, and the development and use of relevant training. Select accomplishments over the past year include:

- The number of active users on the CIKR ISE's delivery platform—Homeland Security Information Network - Critical Sectors (HSIN-CS)—grew by 67 percent; on average, a new user registers for HSIN-CS every 1.5 hours.
- By the end of the second quarter of 2011, HSIN-CS contained 12,250 documents available to users, a 100 percent increase in the number of documents that were available in 2010.
- HSIN Connect, a Webinar tool, hosted more than 28 educational events for approximately 17,500 critical infrastructure stakeholders on topics such as critical infrastructure resilience, threat detection, protective actions, and specific methodologies or critical infrastructure tools.
- Daily open-source infrastructure reports, which provide mission partners with situational awareness and information to assist with their operational planning, were accessed 371,843 times.

Key Initiatives and Activities

CIPAC has been utilized over the past year to support three major initiatives that reflect the maturation of the critical infrastructure mission. The cross-sector councils have been integral in guiding the development of the Critical Infrastructure Risk Management Enhancement Initiative (CIRMEI), an NPPD/IP-led effort to better drive and track the Nation's progress in implementing infrastructure risk mitigation measures. CIPAC has supported NPPD/IP's efforts to assess how it could further tailor its programs to meet the regional needs of its partners. Four SCCs are piloting a tool that permits them to share suspicious activity reports with the Federal Government and critical infrastructure owners and operators. In addition, sector-specific information on these major initiatives is included in the sector chapter, as appropriate.

Critical Infrastructure Risk Management Enhancement Initiative

The CIRMEI will ensure that risk management activities under the NIPP are developed and executed considering risks to critical infrastructure, and that the risk environment and current state of critical infrastructure protection and resilience directly inform programmatic and budgetary planning. As a result of this collaborative effort, NPPD/IP and its partners will be better equipped to base decisions on risk

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

and performance and to achieve desired protection and resilience outcomes. The initiative will lead to the increased coordination of risk management activities within NPPD/IP and across the NIPP partnership.

The CIRMEI drives an enhanced process for measuring progress and assessing the state of critical infrastructure protection and resilience efforts through improved reporting and action-oriented planning. CIPAC has been leveraged to begin guiding the development of the three core elements of the CIRMEI:

- **National Risk Profile (NRP)**: The NRP provides an annual outlook of the landscape of risks facing the critical infrastructure protection and resilience community. The NRP supports strategic planning efforts by broadly identifying the risks facing critical infrastructure (looking forward) and highlighting areas where the risk landscape has changed or the government's understanding of specific risks has improved. The analysis contained in the NRP is meant to help government and private sector decisionmakers understand the critical infrastructure risk landscape and the risks to be managed.
- **National Critical Infrastructure Protection Annual Report (NAR)**: The framework of the NAR has been revised so that it clearly articulates how the programs and initiatives undertaken under the NIPP partnership are making critical infrastructure more secure. The revised framework ensures that the NAR addresses the Homeland Security Act of 2002's demand for a comprehensive measurement of risk to critical infrastructure. The NAR measures the effectiveness and progress of critical infrastructure protection and resilience efforts by Federal, State, local, tribal, and territorial governments and the 18 sectors through a set of outcome statements and associated metrics. These outcome-based metrics will enable the critical infrastructure community to better assess where it is versus where it ought to be in terms of risk management.
- **Critical Infrastructure Risk Management Plan (CIRMP)**: The CIRMP is a collaborative action plan that will address risk reduction opportunities related to critical infrastructure. The CIRMP will describe planned approaches for improving critical infrastructure protection and resilience in areas where progress has been insufficient, based on the findings reported in the NAR and the status of the associated outcome statements. The CIRMP will include milestones that can be used to track implementation progress, as appropriate.

Integration of the NAR and the CIRMP will remain a priority for CIPAC in the year ahead and will inform resource allocation decisions so that resources are applied to areas of the critical infrastructure mission where they are most needed.

Regional Initiative

The National Protection and Programs Directorate's Office of Infrastructure Protection established the Regional Initiative in the spring of 2011. The initiative is designed to identify on a regional level the capabilities and associated programs that NPPD/IP's government and industry partners deem necessary to effectively manage risk to critical infrastructure. Based upon this information, NPPD/IP will deliver voluntary tools to the 10 Federal Emergency Management Agency (FEMA) Regions in a manner that is tailored to their unique needs and risk landscapes.

Under CIPAC, NPPD/IP has hosted several focus group sessions with owners and operators in FEMA Regions I and II. These focus groups provided owners and operators with an opportunity to share their companies' approaches to security and business continuity, and the extent to which these approaches are informed by Federal programs. In addition, the SLTTGCC engaged State and local government officials in the Northeast to better understand the focus of their critical infrastructure protection programs. The SLTTGCC developed a written report on its findings that has served as the primary government input to the Regional Initiative.

Nationwide Suspicious Activity Reporting Initiative

CIPAC is contributing to the Nationwide Suspicious Activity Reporting Initiative by facilitating coordination and information sharing with owners and operators, and implementing sector-specific procedures and tools designed specifically for critical infrastructure participation in this activity. Two sectors—Transportation Systems (Highway and Motor Carrier Mode) and Commercial Facilities—are piloting the Suspicious Activity Report for Critical Infrastructure Tool, which allows sector stakeholders to share suspicious activity reports within their sector and with the National Infrastructure Coordinating Center.

This approach is leveraging the existing capabilities of the CIKR ISE to increase cross-sector visibility of potential threats that may pertain to sector stakeholders. Additional sectors are scheduled to implement the Suspicious Activity Report for Critical Infrastructure Tool in the fall of 2011.

The DHS National Protection and Programs Directorate's Office of Infrastructure Protection offers a wide array of no-cost training programs and resources to government and private sector partners. These Web-based classroom courses and training materials provide government officials and critical infrastructure owners and operators with the knowledge and skills needed to implement critical infrastructure protection and resilience activities. For more information, visit http://www.dhs.gov/files/training/training-critical-infrastructure-partners.shtm.

Path Forward

CIPAC provides an opportunity for government and owners and operators to work together to advance the Nation's critical infrastructure protection and resilience posture. Sustainment of such collaboration is vital, because the risk to critical infrastructure is constantly evolving. Accordingly, the sectors and cross-sector councils have identified a number of priorities for 2012, including continued advancement of the initiatives introduced in "Key Initiatives and Activities," above. In addition, the 18 critical sectors will prioritize the following activities over the next year:

- Improving awareness of interdependencies among sectors and agencies to help identify and address cross-sector infrastructure protection gaps.
- Leveraging existing channels of communication and building additional channels through State and local partnerships with infrastructure owners and operators.
- Expanding the use of metrics to measure program effectiveness and encourage progress toward critical infrastructure protection and resilience goals.
- Disseminating products and training developed by the critical infrastructure partnership to an increasing number of infrastructure owners and operators across the Nation.
- Expanding participation in the critical infrastructure information-sharing processes and improving information-sharing effectiveness and efficiency through the development of standardized requirements linked to specific missions.

CIKR CROSS SECTOR COUNCIL

Partnership

The Critical Infrastructure and Key Resources (CIKR) Cross Sector Council (the Council) leads and coordinates activities to address cross-sector issues and interdependencies among the Sector Coordinating Councils (SCCs) and their member companies and organizations. The Council is comprised of the leadership of each of the SCCs, and the Partnership for Critical Infrastructure Security (PCIS) provides representation for the Council.

Council activities include providing senior-level, cross-sector strategic coordination within private sector critical infrastructure and through partnerships with U.S. Department of Homeland Security (DHS) and the Sector-Specific Agencies. The Council also supports and participates in the development and implementation of the National Infrastructure Protection Plan (NIPP) and the Sector-Specific Plans. The Council is active in identifying, supporting, and raising awareness regarding the interdependencies between sectors; facilitating improved information sharing within the private sector and with the government; and identifying and disseminating best practices for critical infrastructure protection, preparedness, and resilience across sectors and the critical infrastructure community.

Vision

Facilitate 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 increase collaboration among SCCs and the government:

- ***Partnership leadership***: Provide proactive leadership to leverage the partnership model to facilitate private cross-sector collaboration with the government.
- ***Cross-sector leadership***: Provide leadership to identify cross-sector and interdependency risks and recommend approaches to assess and manage those risks.
- ***Sector assistance***: Provide leadership to strengthen SCCs and enhance the role of the partnership framework and collaborate to improve the protection, preparedness, and resilience of the critical infrastructure community.
- ***Effectiveness***: Improve communication and outreach among sectors and with the government, including regular interaction between the Council and the Federal Senior Leadership Council (FSLC).

Selected Accomplishments

The Council's recent accomplishments include:

- Coordinated efforts with government partners through the Cross-Sector Cyber Security Working Group to improve and enhance the U.S. national cybersecurity profile.
- Participated in the development of the National Cyber Incident Response Plan and testing of national cyber preparedness and resilience through the Cyber Storm National Exercise series.
- Examined cybersecurity risk management while raising the awareness of cyber issues and their cross-sector impacts and interdependencies.
- Produced an interim Interdependencies Report that included a MindMap exercise, which demonstrated the critical interdependencies of various sectors based on a study utilizing subject matter experts in four test sectors—Communication, Transportation Systems (Highway-Motor Carrier), Information Technology, and Energy (Oil and Natural Gas and Electricity).
- Participated in the National Level Exercise (NLE) Program, including leadership roles with the NLE 2011 Coordinating Committee and the National Private Sector Working Group (NPSWG); NLE 2011 simulated a catastrophic earthquake event in the New Madrid Seismic Zone area of the United States.
- Worked with several sectors to produce lifelike, ground truth documents to inform the National Exercise Scenario Working Group.
- Provided leadership to each of the NPSWG sub-working groups and populated a private sector simulation cell during the functional exercise to act as a liaison and coordinate with government and private sector partners during the exercise.
- Participated in joint meetings with the FSLC.
- Established a working group to collaborate with White House National Security Staff to provide a 30-day review of the overarching principles of Homeland Security Presidential Directive-7: Critical Infrastructure Identification, Prioritization, and Protection (HSPD-7).
- Established a working group to collaborate with DHS, The Federal Emergency Management Agency, and the White House National Security Staff to contribute to the implementation of the requirements associated with Presidential Policy Directive-8: National Preparedness (PPD-8).
- Enhanced collaboration between the PCIS; the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC); the Regional Consortium Coordinating Council (RCCC); the National Council of Information and Analysis Centers; and other stakeholders.
- Participated in five Joint Critical Infrastructure Partnership regional symposiums as a steering committee member and provided an update about the Council's mission and key initiatives at each symposium.

Key Initiatives

The Council organizes its efforts through several committees made up of member representatives:

- ***Cross-Sector Cyber Security Working Group***: Develops collaborative approaches for improving the Nation's cybersecurity and is chaired by the Council and DHS, under the Critical Infrastructure Partnership Advisory Council framework.
- ***Communications & Outreach Committee***: Enhances internal and external education, awareness, and outreach efforts regarding protection, preparedness, and resilience of critical infrastructure; coordinates online presence to provide links to reports and other deliverables as well as information about Council activities; develops materials to raise awareness across sectors about issues and activities of interest and relevance to members; and educates and informs external partners about the partnership framework and collaborative efforts between private sector owners and operators and the government to improve the protection, preparedness, and resilience of the Nation's critical infrastructure.
- ***National Level Exercise Committee***: Leads and coordinates the private sector critical infrastructure community to design, plan, and implement efforts associated with the execution of national level exercises, including the NLE, Cyber Storm, and the Resilient Constellation series.
- ***Interdependencies Committee***: Identifies and increases understanding of interdependencies within the critical infrastructure community and fosters better communication and collaboration between sectors, their members, and organizations.
- ***Regional, State, and Local Information Sharing Committee***: Helps create security and all-hazards information-sharing networks at the regional, State, and local levels; and assists with the coordination of information sharing between National, regional, State, and local entities.
- ***Engagement Working Group***: Works with the DHS National Protection and Programs Directorate's Office of Infrastructure Protection to examine processes and protocols for the sharing of timely and relevant threat information.
- ***Homeland Security Presidential Directive-7: Critical Infrastructure Identification, Prioritization, and Protection (HSPD-7) Working Group***: Provides a high level review of the overarching principles associated with HSPD-7 to determine whether any revision, updates, or refresh should be considered.
- ***Presidential Policy Directive-8: National Preparedness (PPD-8) Working Group***: Works with DHS, FEMA, and the White House National Security Staff to develop and implement the requirements identified in PPD-8: National Preparedness.
- ***Reboot Initiative***: Conducts an internal assessment to determine whether the PCIS mission, goals, and objectives remain current or require any revisions or updates to continue to meet the collaborative objectives of the NIPP.

Path Forward

Important upcoming activities for the Council include:

- Continue the important work of the Interdependencies Committee and finalize the Sector Interdependencies Report.
- Actively engage with the design and implementation of the National Preparedness Goal and National Preparedness System as required by PPD-8.
- Continue to build out the participation of the private sector critical infrastructure community in the design, planning, and implementation of NLE to test the Nation's preparedness and resilience.
- Facilitate efforts to enhance the collaboration between the private sector, critical infrastructure community, and the U. S. Government.
- Address important issues such as access and credentialing challenges regarding incident response and consequence management; and coordination of communication and efforts related to pending or potential threats and risk to the Nation's critical infrastructure.
- Enhance and expand efforts with other stakeholders, including the SLTTGCC, RCCC, National Council of Information and Analysis Centers, and others, to improve the protection, preparedness, and resilience of the Nation's critical infrastructure.
- Expand communications and outreach activities for our internal and external partners and stakeholders.
- Work with our government partners to execute the partnership framework to meet the goals and objectives of the NIPP.

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 Systems – Aviation Mode
- Transportation Systems – Highway and Motor Carrier Mode
- Transportation Systems – Mass Transit Mode
- Transportation Systems – Pipeline Mode
- Transportation Systems – Railroad Mode
- Water

FEDERAL SENIOR LEADERSHIP COUNCIL

Partnership

The National Infrastructure Protection Plan (NIPP) Federal Senior Leadership Council (FSLC) was formed to enhance communication, collaboration, and coordination among Federal departments and agencies with a role in implementing the NIPP and Homeland Security Presidential Directive-7: Critical Infrastructure Identification, Prioritization, and Protection (HSPD-7). FSLC members include the Sector-Specific Agencies (SSAs) for each critical infrastructure sector as well as several additional agencies named in HSPD-7. The FSLC is one of two subcouncils of the Government Cross Sector Council, along with the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC).

Key Activities

The FSLC 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 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 in the Sector Critical Infrastructure Protection Annual Reports (SARs) and the National Critical Infrastructure Protection Annual Report (NAR).

Selected Accomplishments

Recent accomplishments of FSLC agencies include the following:

- Worked with government and private sector partners to implement individual SSPs, with emphasis on resilience and interdependencies, as appropriate to each sector.
- Collaborated on the Critical Infrastructure Risk Management Enhancement Initiative (CIRMEI) with State, local, tribal, and territorial (SLTT) government partners and critical infrastructure owners and operators to improve protection and resilience efforts.
- Participated throughout the year in cross-sector teleconferences and Webinars with U.S. Department of Homeland Security, SLTT governments, and private sector critical infrastructure partners to discuss new and evolving threats to critical infrastructure security.
- Contributed to development of the National Coordinator, SLTT, and sector outcome statements and metrics, designed to enable more robust measurement and reporting of progress in improving critical infrastructure protection and resilience.
- Conducted two joint meetings with the SLTTGCC, the Critical Infrastructure and Key Resources Cross Sector Council, and the Regional Consortium Coordinating Council.
- Developed the 2011 SARs and contributed to development of the 2011 NAR.
- Participated, through the Critical Infrastructure Protection and Resilience Interagency Policy Committee, in the development, review, and implementation plan for Presidential Policy Directive-8: National Preparedness.

Membership

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

Sector-Specific Agency	Critical Infrastructure Sector
Department of Agriculture[a] Department of Health and Human Services[b]	Food and Agriculture
Department of Defense[c]	Defense Industrial Base
Department of Energy	Energy[d]
Department of Health and Human Services	Healthcare and Public Health
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Water[e]
Department of Homeland Security *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[f]
Transportation Security Administration	Postal and Shipping
Transportation Security Administration, United States Coast Guard[g]	Transportation Systems[h]

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

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

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

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

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

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

g. The U.S. Coast Guard is the SSA for the Transportation Systems – Maritime Mode.

h. 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.

OTHER 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 Justice
- U.S. Department of State
- U.S. Department of Transportation

STATE, LOCAL, TRIBAL, and TERRITORIAL GOVERNMENT COORDINATING COUNCIL

Partnership

The State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC), established in April 2007, strengthens the National Infrastructure Protection Plan (NIPP) sector partnership by integrating State, local, tribal, and territorial (SLTT) governments into the national critical infrastructure planning process. SLTTGCC members offer broad institutional knowledge from a wide range of professional disciplines related to critical infrastructure protection and resilience. The SLTTGCC is one of two subcouncils of the Government Cross-Sector Council (the other is the Federal Senior Leadership Council (FSLC)), and addresses wide-ranging infrastructure protection and resilience issues across all 18 critical infrastructure sectors through the sector Government Coordinating Councils (GCC).

The SLTTGCC currently has 42 members representing a wide array of jurisdictions who seek to integrate diverse perspectives, priorities, and needs from the SLTT community into a unified critical infrastructure protection and resilience mission. State representatives constitute the largest plurality of the SLTTGCC membership, which also includes representatives from county, municipality, tribal, and territorial governments. The SLTTGCC also engages numerous subject matter experts to broaden and inform its perspectives on select issues of importance to the critical infrastructure protection and resilience mission.

The SLTTGCC integrates multidisciplinary perspectives through its involvement in the NIPP partnership. Government critical infrastructure stakeholders participating in the SLTTGCC include homeland security advisors, law enforcement officials, critical infrastructure coordinators, public health officials, emergency managers, fire services representatives, information security officials and State water officials. The Council adds representation from additional State information security officers, as well as transportation or port authority representation when possible. SLTTGCC members serve as liaisons to sector GCCs, representing SLTT perspectives at GCC and joint GCC/Sector Coordinating Council meetings.

Vision

The Council's vision is to stimulate dialogue between all levels of government to fulfill the critical infrastructure protection and resilience mission.

Goals

Protection and resilience goals support the overall SLTGCC strategic planning process:

- Ensure that SLTT homeland security officials or their designated representatives are integrated as active participants in national critical infrastructure protection and resilience efforts.
- Encourage the integration of SLTT government perspectives into Federal planning efforts and promote 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 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

The Council's accomplishments over the past year include the following:

- Authored the report, *Federal Critical Infrastructure Programs Review and Federal Critical Infrastructure Programs Review: Next Steps*, which offers the SLTTGCC strategic analysis and recommendations for enhancing the value of programs sponsored by the National Protection and Programs Directorate's Office of Infrastructure Protection for SLTT stakeholders.
- Produced *Landscape of State and Local Government Critical Infrastructure Resilience Activities and Recommendations*, the first report of its kind to document how State and local governments approach infrastructure resilience; the report includes recommendations to DHS on steps to foster greater national resilience.
- Authored *Landscape Report: State Entities Participating in a Public-Private Partnership Environment*, which examines State sunshine laws and critical infrastructure stakeholder information sharing.
- Published the *Regional Partnerships and the Critical Infrastructure Protection and Resilience Mission*, which provides actionable information for SLTTs to utilize when considering whether to join or form a regional partnership to facilitate the integration of critical infrastructure security, preparedness, and resilience programs and activities.
- Updated the *CIKR Partnerships: State Characteristics and Capabilities (Version #2)* study, which summarizes the characteristics of partnerships and activities implemented to achieve protection, readiness, and resilience mission goals; the summaries provide a resource of State and local best practices across the Nation.
- Participated in five Joint Critical Infrastructure Partnership regional symposiums as a steering committee member and provided an update about the council's mission and key initiatives at each symposium.

Key Initiatives

The SLTTGCC holds biannual in-person plenary sessions. Between these sessions, the Council conducts most of its activities through seven working groups:

- Access Credentialing Working Group
- Program Review Working Group
  - Automated Critical Asset Management System Sub Working Group
  - Chemical Facility Anti-Terrorism Standards Sub Working Group
- Homeland Security Advisor Working Group
- Information Sharing Working Group

- Policy and Planning Working Group
- Regional Resiliency Assessment Program Working Group
- Tribal and Territorial Working Group

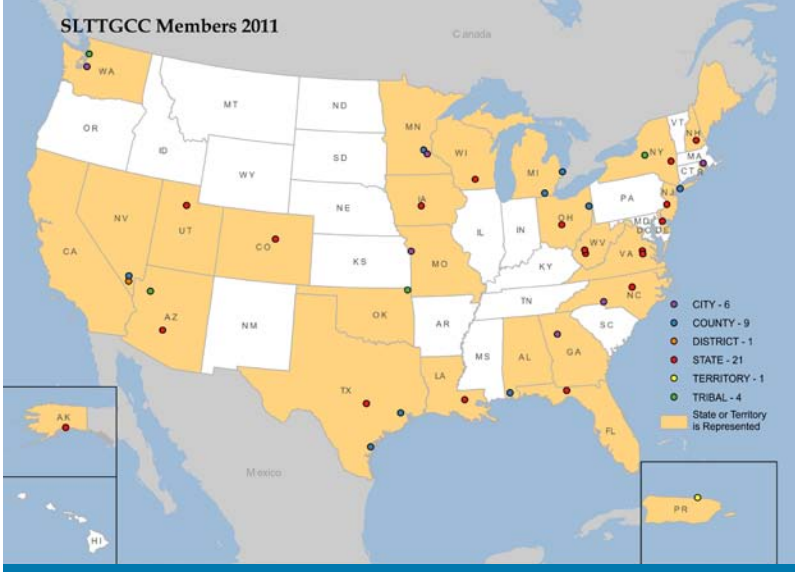
Over the past year, the SLTTGCC supported two initiatives: the National Protection and Programs Directorate/Office of Infrastructure Protection (NPPD/IP) Regional Initiative and a series of NPPD/IP-sponsored infrastructure protection and resilience-focused Webinars. These initiatives were designed to advance and mature the national critical infrastructure mission and NPPD/IP's stewardship of that mission, as elucidated below.

- ***Regional Initiative***: To better serve its constituency of SLTT government officials and to assist DHS in providing effective programs to its partners in the field, the SLTTGCC is collecting and analyzing State and local government requirements for managing risk to critical infrastructure. The Council is conducting facilitated sessions with government officials in each Federal Emergency Management Agency (FEMA) Region (e.g., State critical infrastructure protection coordinators, urban area working group personnel, and local government officials) to gather critical infrastructure requirements. This outreach began with FEMA Regions I and II and will proceed to the remaining eight FEMA Regions. The Council's Interim Report: Northeast Region was provided to the Assistant Secretary for Infrastructure Protection in August. In the interim report, the SLTTGCC examines the status of critical infrastructure protection programs and activities in eight northeast States. Input from the initiative's data collection and the interim report will form the basis for a final SLTTGCC report to be submitted to DHS, detailing partner requirements and recommendations for programmatic enhancements.
- ***Webinars***: In collaboration with NPPD/IP, the SLTTGCC is hosting a series of Webinars that create a continuous flow of information about both new and existing programs from DHS to SLTT critical infrastructure stakeholders. Webinars create a forum for participants to reinforce doctrine, share updates, and explore best practices with those utilizing the tools and programs in the field. Stakeholders have the opportunity to ask questions and address concerns with programs.

Path Forward

In the coming year, the SLTTGCC will continue to advance critical infrastructure protection and resilience guidance, strategies, and programs, including the following:

- Engage SLTT partners in each FEMA Region to understand their requirements for implementing critical infrastructure risk management programs, current capabilities, resources, and operating structure.
- Broaden and diversify its pool of members and subject matter experts.
- Encourage the integration of regional perspectives into the NIPP partnership framework.
- Advocate consensus-built requirements to address gaps in information sharing.
- Ensure effective SLTT representation on the critical infrastructure sector councils.
- Continue to evaluate the Homeland Security. Information Network-Critical Sectors (HSIN-CS) as a communication vehicle for SLTTGCC use and recommend improvements.
- Focus on the full integration of the NIPP into an all-hazards environment.
- Contribute to the successful implementation of the Presidential Policy Directive-8: National Preparedness.



SLTTGCC MEMBERS

- Alaska Division of Homeland Security and Emergency Management
- Arizona Department of Homeland Security
- Atlanta Police Department
- Bloomington, Minnesota Fire Department
- California Emergency Management Agency
- Charlotte, North Carolina Fire Department
- City of Seattle
- Clark County, Nevada Office of Emergency Management and Homeland Security
- Colorado State Police, Office of Preparedness and Security
- Columbiana County, Ohio Health District
- Delaware Department of Safety and Homeland Security
- Florida Department of Law Enforcement
- Georgia Emergency Management Agency
- Government of Puerto Rico, State Homeland Security Office
- Harris County, Texas Office of Homeland Security and Emergency Management
- Hennepin County, Minnesota Department of Human Services and Public Health
- Hualapai Nation Police Department
- Iowa Homeland Security and Emergency Management Division
- Kansas City, Missouri Police Department
- Lenawee County, Michigan Office of Homeland Security and Emergency Management
- Louisiana Governor's Office of Homeland Security and Emergency Preparedness
- Maine Emergency Management Agency
- Miami Nation Department of Public Safety
- Mobile County, Alabama Sherriff's Office
- Nassau County, New York Department of Health, Office of Public Health Preparedness
- New Hampshire Department of Safety
- New Jersey Office of Homeland Security and Preparedness
- New York State Office of Homeland Security
- North Carolina Department of Crime Control and Public Safety
- Nueces County, Texas Office of Emergency Management
- Ohio Department of Public Safety
- Oneida Indian Nation Police Department
- Providence, Rhode Island Emergency Management Agency and Office of Homeland Security
- Southern Nevada Health District
- St. Clair County, Michigan Office of Emergency Management/Homeland Security
- Texas Office of Homeland Security
- Tulalip Tribal Police Services
- Utah Department of Public Safety
- Virginia Department of Health
- Virginia Governor's Office of Commonwealth Preparedness
- West Virginia Critical Infrastructure Protection Task Force
- West Virginia Office of Homeland Security/ Emergency Management
- Wisconsin Office of Justice Assistance

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, U.S. Department of Homeland Security (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 NIPP. These activities may include enhancing the 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.

The RCCC seeks to understand, connect, enable, and build partnerships to enhance the protection of the critical infrastructure of the United States and the resilience of our communities. Currently, the RCCC has 23 members that represent 39 States and nine metropolitan areas.

Vision

Fully integrate regional consortia into critical infrastructure protection strategies to enhance the safety, security, and resilience of critical infrastructure nationwide.

Goals

The RCCC 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 the 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 Partnership 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 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 Critical Infrastructure Partnership Advisory Council to evaluate regional interdependencies between critical infrastructure sectors that specifically impact RCCC member entities.
- Assess effective security and other preparedness measures of regional consortia and their member entities and incorporate them, as appropriate, into a Council inventory 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 RCCC accomplishments include the following:

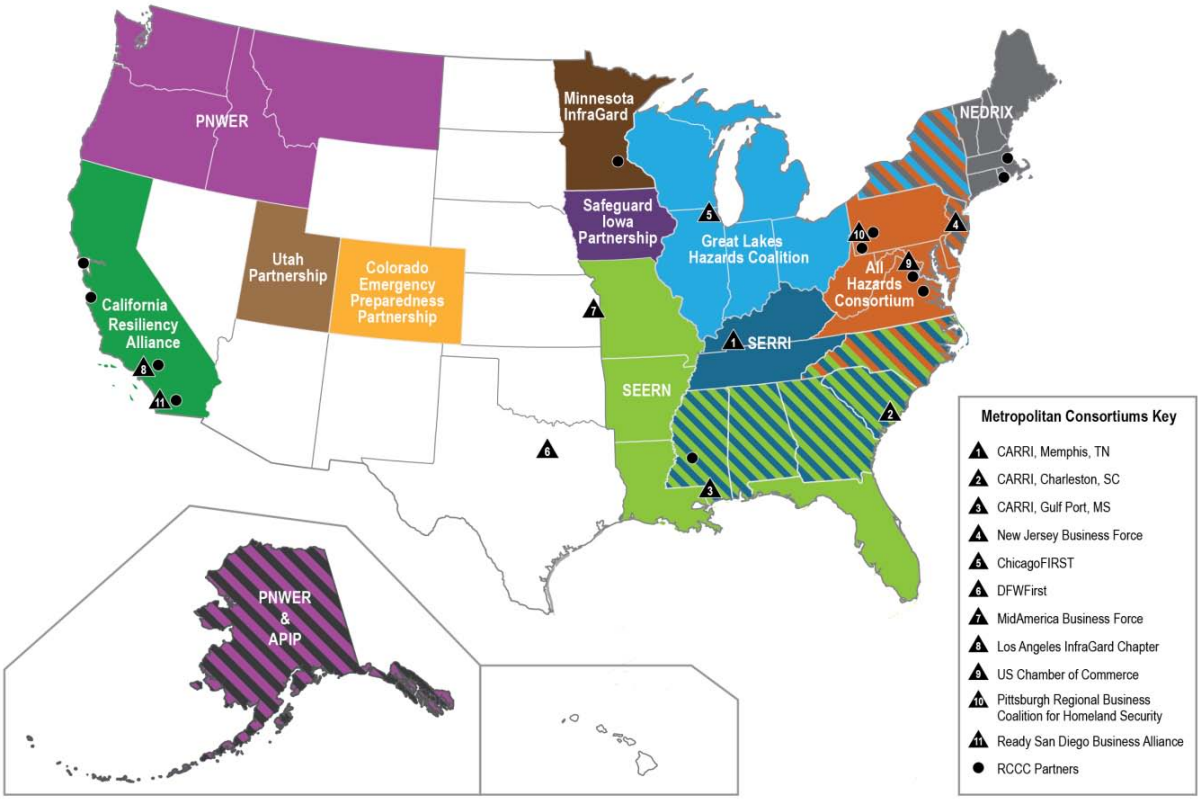
- Completed the *Regional Partnerships: Enabling Regional Critical Infrastructure Resilience* study, which focused on the role of regional partnerships in critical infrastructure protection and resilience.
- Hosted the 2011 Annual Regional Consortium Coordinating Council Plenary.
- Participated in five Joint Critical Infrastructure Partnership regional symposiums as a steering committee member and provided an update about the Council's mission and key initiatives at each symposium.

Key Initiatives

The RCCC is engaged in various initiatives to advance critical infrastructure protection, vulnerability reduction, and consequence mitigation, including the following:

- Partnering with the Critical Infrastructure and Key Resources (CIKR) Cross Sector Council and State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) to improve information sharing and communication throughout the Sector Partnership Framework.
- Hosting Webinars to enhance understanding of the RCCC, the CIKR Cross Sector Council, and the SLTTGCC roles in critical infrastructure protection and resilience. Identify ways in which the three councils can leverage one another.
- Conducting regional catastrophic event response and recovery exercises in conjunction with existing regional workshops.
- Identifying best practices and standards for the use of social media tools in critical infrastructure protection and resilience.
- Developing a communication and collaboration strategy that embraces social technology and employs controls and practices that are efficient, effective and commensurate with the emerging risk environment.
- Aiding in the development and coordination of State and local Critical Infrastructure Asset Registries.

Regional Consortium Coordinating Council Map Of Participants



Path Forward

The RCCC developed an aggressive plan to accelerate its maturation throughout 2011 and 2012. Steps that will be taken as the RCCC moves forward in achieving its goals include the following:

- Reaching out to the critical infrastructure community as a whole.
- Identifying additional regional partnership activities.
- Focusing on interregional dependencies.
- Sharing the findings of the regional resilience roadmap.
- Continuing to build the structures that will enable the RCCC to assist with national-level policy discussions that affect regional critical infrastructure entities, owners, and operators.

"Effective regional partnership can provide a trusted environment for jurisdictions to exchange information, identify common problems, and collaborate on shared goals. Regional partnerships can serve as the "convener," bringing together and provided a level playing field for disparate jurisdictions."

Source: 2011 Regional Partnerships: Enabling Regional Critical Infrastructure Resilience Study

"A regional resilience and overarching risk management focus promotes closer collaboration, integration, and coordination among stakeholders in regions across the country."

Source: 2011 Regional Partnerships: Enabling Regional Critical Infrastructure Resilience Study

RCCC MEMBERS

- Alaska Partnership for Infrastructure Protection
- All Hazards Consortium
- California Resiliency Alliance
- ChicagoFIRST
- Colorado Emergency Preparedness Partnership
- Community and Regional Resilience Institute, Charleston, SC
- Community and Regional Resilience Institute, Gulfport, MS
- Community and Regional Resilience Institute, Memphis, TN
- Dallas-Fort Worth FIRST
- InfraGard Los Angeles
- Great Lakes Hazards Coalition
- Mid-America Business Force
- Minnesota InfraGard
- New Jersey Business Force
- Northeast Disaster Recovery Information X-Change
- Pacific Northwest Economic Region
- Pittsburgh Regional Business Coalition for Homeland Security
- Ready San Diego Business Alliance
- Safeguard Iowa
- Southeast Emergency Response Network
- South East Regional Research Initiative
- U.S. Chamber of Commerce
- Utah Partnership

BANKING AND FINANCE SECTOR

Partnership

The Banking and Finance Sector is essential to facilitating world economic activity. The partnership's private sector members are represented by 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 for Financial Industry Resilience, Security, and Teamwork (RPC*first*). These private sector entities connect key executives and experts throughout the sector. The public sector members form the Financial and Banking Information Infrastructure Committee (FBIIC). The U.S. Department of the Treasury is the Sector-Specific Agency (SSA) for the Banking and Finance Sector.

Vision

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

Goals

The following goals were developed in support of the sector's vision and help provide the basis for ongoing risk management activities:

- Achieve the best possible position in the face of myriad 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 and intelligence communities, financial regulatory authorities, the private sector, and international counterparts to address threats facing the Financial Services Sector.

Selected Accomplishments

Sector partners have taken measures over the past year to increase the sector's security and resilience posture. The sector's accomplishments include the following:

- Developed the Financial Services Threat Matrix that addresses impacts to market and institutional confidence, concentration, supply chain, infrastructure, geographic proximity, and technology risks.
- Enhanced cybersecurity information sharing.
- Engaged in multiple FS-ISAC and regional exercises, and assisted with coordinated crisis response planning by developing an All Hazards Crisis Response Playbook.
- Participated in the U.S. Department of Homeland Security (DHS) Cross-Sector Cybersecurity Working Group, which reviews cross-sector cybersecurity strategies and programs.
- Leveraged the security clearances provided by the Federal Government to senior executives in the Banking and Finance Sector through a series of briefings.
- Completed a memorandum of understanding on cybersecurity research in conjunction with the White House, DHS, and the National Institute of Standards and Technology and initiated a cooperative research agreement to improve the accuracy, timeliness, and cost effectiveness of the identity proofing process.
- Collaborated with White House officials on the *National Strategy for Trusted Identities in Cyberspace.*
- Provided input on the *National Cyber Incident Response Plan.*

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:

- Identifying future operational challenges for the sector through a "long-range vision" effort to ensure that infrastructure owners and operators continually position themselves for a rapidly evolving threat environment.
- Developing a prioritized threat matrix covering the Financial Services Sector that provides shared insight and focused expertise into the opportunities and requirements for initiatives that address current and projected threats to the Banking and Finance Sector.
- Increasing focus on cybersecurity threats to assist financial sector firms with mitigating the risks posed by cyber criminals and nation states.
- Conducting critical sector exercises to test the sector's emergency protocols for sharing information, escalating where appropriate, and deciding on courses of action in the response to potential events.
- Building strong and clear lines of communication across sector entities by establishing viable relationships and formal protocols in advance of an event and testing core capabilities at every opportunity (real-world and scheduled exercises).

"The protective programs range from developing and testing robust emergency communication protocols, to identifying critical Financial Services Sector threats, to addressing cybersecurity threats and risk mitigation strategies. The success of the public-private partnership has proven critical to the Financial Services Sector's achievements through one of the most challenging periods for the sector with respect to credit and liquidity risks."

Source: 2011 Banking & Finance Sector Annual Report

"...the threat environment has evolved in the past several years posing challenges at an individual firm, sector and national level and in response the FSSCC and FS-ISAC have seen significant membership activity. The sector's ability to coordinate among member firms, associations, other sectors and government regulators and agencies has improved as a result."

Source: 2011 Banking & Finance Sector Annual Report

- Boosting efforts in research and development, especially efforts to enhance identity management and understanding insider threats.
- Embedding FS-ISAC staff within DHS in the National Infrastructure Coordinating Center and National Cybersecurity and Communications Integration Center.
- Increasing coordination among intelligence agencies, regulators, other government agencies, and the private sector.
- Leading coordinated responses to crises, including hurricanes, pandemic flu, and earthquake/tsunami situations.

Path Forward

The Banking and Finance Sector is undertaking a number of activities to enhance the protection and resilience of its assets, including the following:

- Enhance information sharing and coordination.
- Integrate the sector's Threat Analysis Tool in risk management and contingency plans.
- Conduct exercises and training.
- Invest in research and development.
- Coordinate efforts internationally.
- Address supply chain risks and financial top level domain concerns.
- Provide expert advice on cybersecurity policy issues.
- Ensure continuity of leadership and expanding participation of private sector partners.
- Continue senior leadership meetings between the FSSCC and FBIIC at least three times a year.
- Improve identity proofing through the joint government-FSSCC pilot effort, Financial Institution – Verifying Identity Credentials Services, and work with the Treasury Department to consolidate and prioritize efforts.
- Increase committee membership and focusing on the FSSCC's international functional area and related efforts across the sector.

"The Financial Services Sector intends to leverage this year's work on the Threat Matrix to identify the top threats and risks to focus on going forward. The disciplined approach to identifying, prioritizing, and organizing threats into the Financial Services Sector critical infrastructure is intended to service as a foundation for managing the sector's strategy for years to come."

Source: 2011 Banking & Finance Sector Annual Report

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 Association of Insurance Commissioners
- National Association of State Credit Union Supervisors
- National Credit Union Administration
- North American Securities Administrators Association
- Office of the Comptroller of the Currency
- Securities and Exchange Commission
- Securities Investor Protection Corporation
- U.S. Department of the Treasury

FSSCC MEMBERS

The FSSCC has 52 member associations and financial institutions representing:

- Clearinghouses
- Commercial banks
- Credit rating agencies
- Exchanges/electronic communication networks
- Financial advisory services
- Insurance companies
- Financial utilities
- Government-sponsored enterprises
- Investment banks
- Merchants
- Retail banks
- Electronic payment firms

CHEMICAL SECTOR

Partnership

The Chemical Sector—with its nearly 1 million employees and annual revenues between $600 billion and $700 billion—is an integral component of the U.S. economy. This sector converts raw materials into more than 70,000 products, many of which are critical to the Nation. The U.S. Department of Homeland Security (DHS) is responsible for managing and coordinating Chemical Sector security activities in accordance with Homeland Security Presidential Directive-7: Critical Infrastructure Identification, Prioritization, and Protection. This overarching responsibility has been delegated to the DHS National Protection and Programs Directorate's Office of Infrastructure Protection (NPPD/IP). The Chemical Sector-Specific Agency (SSA), which oversees these voluntary efforts under the National Infrastructure Protection Plan (NIPP), resides within the NPPD/IP Sector-Specific Agency Executive Management Office, Chemical Branch. The SSA operates under the 2009 NIPP Partnership Framework, which establishes a collaborative link between private sector partners and Federal, State, local, tribal, and territorial partners. The Federal partners engaged in chemical security are represented on the Chemical Government Coordinating Council (GCC). As the owners of critical infrastructure in the sector, private sector partners, who are represented through the Chemical Sector Coordinating Council (SCC), are vital to the sector's protection and resilience efforts. The Infrastructure Security Compliance Division was established within the NPPD/IP to administer the Chemical Facility Anti-Terrorism Standards (CFATS).

A fundamental objective of the 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 possible disruptions in critical systems.

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 have also adopted measures to enhance the 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 consider all hazards, incorporate a greater focus on resilience, address cybersecurity, and ensure greater alignment with sector programs and activities. The sector's overarching goals are as follows:

- 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/private sector coordination to increase sector resilience, as necessary.
- Support risk-based critical infrastructure protection research and development 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:

- Continued implementation of the CFATS regulating facilities deemed the highest risk in the sector (as of August 12, 2011, 3,951 facilities have been assigned a final tier and, currently, 618 are awaiting a final tier assignment).

"VCAT [Voluntary Chemical Assessment Tool] has proved to be very, very beneficial to us, as finding vulnerabilities and helping to put systems, and plans or procedures in place to address those vulnerabilities. I would strongly encourage you, if you have not signed up and got[ten] on board with VCAT, you should probably do so at your earliest opportunity."

Source: Private sector partner presenting at the 2011 Chemical Sector Security Summit – July 6, 2011

"The Summit was very well done and a good investment of my time."

Source: Private sector partner attending the 2011 Chemical Sector Security Summit – July 7, 2011

"The exercise was very thorough, content was detailed and provided room for discussion, and there were good resources for the presentation."

Source: Private Sector partner attending the State Security Seminar & Exercise Series held – March 31, 2011

"I will use the materials to improve situational awareness at my facility. Improvised Explosive Device (IED) inner workings was very informative and useful for our facility security effort. [We] will use [the] information to improve surveillance/detection measures."

Source: Private sector partner attending the Chemical Sector Explosives Threat Awareness Training held on April 20, 2011

- Coordination of the fifth annual Chemical Sector Security Summit in July 2011, which had a record attendance of 521 attendees—78 percent of whom represented industry.
- Certification of 7,785 individuals who completed the Web-based Chemical Security Awareness Training Program (11,198 individuals have completed the training since its launch in July 2008).
- Formation of a Roadmap Implementation Working Group to address milestones set forth in the *Roadmap to Secure Control Systems in the Chemical Sector* through collaborative efforts between the chemical industry, SSA, and the National Cyber Security Division.
- Creation and active distribution of the *Roadmap Awareness Campaign* DVD with training, standards, a cyber tabletop exercise, and an evaluation tool.
- Collaboration on incident management processes and information sharing during Cyber Storm III, an exercise in which players tested their company emergency plans and used the exercise after-action report to inform future planning.
- Participation in a number of information-sharing initiatives, such as refining the standing information needs of the sector and the National Infrastructure Advisory Council's information-sharing study.
- Support of 10 Seminar and Exercise Series events across the country, which focused on an active shooter or vehicle-borne improvised explosive device scenario and had 602 participants from the private sector and emergency responder communities.
- Acceptance of the Voluntary Chemical Asssessment Tool (VCAT) by one of the SCC industry associations that included the tool as one of the security risk assessments under its security program.

Key Initiatives

Sector partners are currently implementing a variety of protective programs to meet security goals. Key initiatives within the sector include:

- Identifying, assessing, and securing high-risk facilities through the implementation of CFATS and the Maritime Transportation Security Act of 2002.
- Improving security practices and raising awareness through private sector security guidance programs, documents, and plans.
- Developing innovative security training and sharing best practice security information for distribution through the collaborative efforts of DHS and several State chemical industry councils.
- Enhancing information sharing through the Chemical Sector Security Summit; the Classified Chemical Sector Briefings; the monthly suspicious activity teleconferences held jointly with the Oil and Natural Gas Sub-Sector; the Chemical Sector Training and Resources Web site on www.dhs.gov; and the Homeland Security Information Network.
- Promoting the VCAT to assist owners and operators in assessing risks associated with their facilities.
- Developing and promoting free, Web-based tools, training, and best practices documents for easy access by all sector partners.
- Raising awareness by providing educational training opportunities through the Ammonia Safety and Training Institute and Transportation Community Awareness and Emergency Response efforts.
- Providing a forum for 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 and developing sector cyber incident management procedures.

Path Forward

As the Chemical Sector moves forward in protecting and enhancing the resilience of its critical infrastructure, the sector will:

- Work with Congress and other security partners to make CFATS a permanent regulatory program for high-risk chemical facilities.
- Encourage an ongoing private-public dialogue through the NIPP partnership framework to improve information sharing on chemical security legislation and harmonize security regulations across the Federal Government.
- Work to minimize the disruption to SCC representation and sector information sharing while implementing Executive Order 13490, Ethics Commitments by Executive Branch Personnel.
- 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.

"That is great and much appreciated. We are holding a Homeland Security Awareness Bootcamp in New Orleans next week and this material will be great for our attendees."

Source: Private sector partner response to receiving digital copies of best practice guides and other resources in the ChemicalSector@dhs.gov inbox

GCC MEMBERS

- Chemical Safety Board
- Office of the Director of National Intelligence
- 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 Justice
- U.S. Department of Labor
- U.S. Department of State
- U.S. Department of Transportation
- U.S. Environmental Protection Agency

SCC MEMBERS

- Agricultural Retailers Association
- American Chemistry Council
- American Coatings Association
- BASF Corporation
- CF Industries, Inc.
- Chemical Producers & 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 Inc.
- Society of Chemical Manufacturers and Affiliates

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 that have differing needs and challenges. The Commercial Facilities Sector also includes facilities and assets (e.g., stadiums, entertainment districts, 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) National Protection and Programs Directorate's Office of Infrastructure Protection serves as the Sector-Specific Agency (SSA) for the Commercial Facilities Sector.

Vision

The Commercial Facilities Sector envisions a secure, resilient, and profitable sector in which effective and non-obstructive risk management programs instill a positive sense of safety and security in the public and sustain favorable business environments that are 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 public and private sector partners at all levels of government.
- Ensure that the public sector 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. The sector's accomplishments over the past year include the following:

- Developed four additional Risk Self-Assessment Tool (RSAT) modules specifically tailored to address risks associated with convention centers, lodging, racetracks, and theme parks and fairgrounds.
- Created a *Protective Measures Guide for the U.S. Lodging Industry.*
- Enhanced information sharing through the development of the Suspicious Activity Reporting (SAR) Tool.
- Conducted seven classified briefings in seven cities across the country.
- Developed *Cybersecurity in the Retail Subsector Webinar* in collaboration with the National Cyber Security Division.
- Held two GCC meetings focusing on resilience.
- Co-sponsored the Cross Sector Supply Chain Working Group.
- Developed the *Active Shooter: What You Can Do* course through the Federal Emergency Management Agency Emergency Management Institute.

"An additional 51 members registered to use the existing [Risk Self-Assessment Tool] modules this year, bringing the total registered users to 127 since October 2009. During this reporting period, 32 out of 43 venues submitted their facility data for analysis, an increase from last year's totals of 11 out of 37 total completions."

Source: 2011 Commercial Facilities Sector Annual Report

Key Initiatives

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

- Providing explicit risk mitigation guidance to owners and operators through DHS hotel and lodging advisory posters, protective measures guides, *Active Shooter: What You Can Do* training materials, pandemic influenza planning documents for public assembly facilities, Building Owners and Managers Association international awareness programs, and the Commercial Facilities SSA outreach program.
- Fostering an educational framework in which risk methodologies can be explored and understood for training purposes 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 RSAT for stadiums and arenas, performing arts centers, lodging, convention centers, racetracks, theme parks, and fairgrounds.
- Developing the Commercial Facilities SAR Tool, which allows commercial facility owners and operators to act as information-sharing force multipliers by providing a platform for SAR to the National Infrastructure Coordinating Center.
- Participating in tabletop exercises that allow participants to focus on key information-sharing and response capabilities through facilitated discussions.

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:

- Work with private and public sector partners for subsector outreach and information sharing through tabletop exercises and other initiatives, concentrating on private sector partners that are less engaged.
- Promote the Protected Critical Infrastructure Information Program to ease the concern that owners and operators share regarding the disclosure of sensitive or proprietary information about assets or security measures to the Federal Government.
- Improve the quality, quantity, and timeliness of actionable threat information that would help facilities identify appropriate responses to potential threats.
- 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.
- Increase the focus on resilience and interdependencies as the Commercial Facilities Sector will explore further involvement in the "Resilience Star" program, which is a voluntary program that recognizes facility resilience.
- Continue to participate in the Regional Resiliency Assessment Program, which evaluates regional critical infrastructure to identify dependencies, interdependencies, cascading effects, resilience characteristics, and gaps.

"The central focus of the Commercial Facilities [Table Top Exercise] series, as part of the Subsector Outreach and Information-Sharing Initiative, is to gauge the effectiveness of information-sharing processes within the public and private sector in the event of a dynamic threat and attack."

Source: 2011 Commercial Facilities Sector Annual Report

GCC MEMBERS

- U.S. Department of Agriculture
- U.S. Department of Commerce
- 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

- Beacon Capital Partners
- Building Owners and Managers Association International
- Cushman & Wakefield
- Georgia World Congress Center
- Home Depot
- International Association of Amusement Parks and Attractions
- International Association of Fairs and Expositions
- International Association of Venue Managers
- International Council of Shopping Centers
- Lowe's
- M Resort Spa Casino

SCC MEMBERS CONTINUED

- Major League Baseball
- Mall of America
- Marriott International
- National Association for Stock Car Auto Racing, Inc.
- National Hockey League
- National Multi Housing Council
- National Retail Federation
- NBC Universal
- Oneida Gaming Commission
- Paramount Pictures
- RBC Center
- Related Management Company
- Retail Industry Leaders Association
- Self Storage Association
- Simon Property Group
- Stadium Management Association
- Starwood Hotels and Resorts Worldwide
- Target
- The Real Estate Roundtable
- Tishman Speyer Properties
- Trump Organization
- Walmart
- Westfield Shopping Centers

COMMUNICATIONS SECTOR

Partnership

Although new Communications Sector technologies and services enhance opportunities for response to and recovery from natural and manmade disasters, interdependencies between the Communications Sector and the Information Technology Sector place an even greater importance on protecting sector assets, systems, and networks. Communications Sector technologies include wireline, wireless, satellite, cable, and broadcasting transport networks that are part of an even larger global infrastructure. These technologies support internet, voice, data, and other key information and communication services. In addition to its strategic importance, 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. The sector symbolizes the cooperation and trusted relationships that have resulted in the delivery of critical services when emergencies and disasters occur. Ownership is diverse in this sector, which is mostly comprised of private companies.

Forty-six private sector organizations and their respective trade associations form the Communications Sector Coordinating Council (SCC), and 11 Federal departments and their agency representatives form the Communications Government Coordinating Council (GCC). The National Communications System (NCS) within the U.S. Department of Homeland Security serves as the Sector-Specific Agency. NCS manages various communications partnerships that aim to improve all-hazards response, promote physical and cybersecurity situational awareness and the exchange of information through the National Coordinating Center for Telecommunications 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. Through collaborative efforts, the sector strives to ensure that no known threats, physical or virtual, present a substantial risk to the national communications infrastructure.

Goals

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

- Protect and enhance the overall physical and logical health of communications.
- Rapidly reconstitute critical communications services 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

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

- Provided recommendations and best practices to ensure the optimal security and reliability of communications systems (including telecommunications, media, and public safety) through the Federal Communication Commission's Communications Security, Reliability, and Interoperability Council.
- Conducted joint exercises and training initiatives including Eagle Horizon and Cyber Storm III, which tested the National Cyber Incident Response Plan.
- Updated collaborative sector documents that include the *2010 Communications Sector-Specific Plan*, the *2011 National Sector Risk Assessmen*t (NSRA), and the *2009 National Emergency Communications Plan.*
- Worked with private sector partners to improve cross-sector coordination mechanisms and to address critical interdependencies, including cybersecurity interdependencies, through the Telecom/Energy Working Group and the Cross-Sector Cybersecurity Working Group.
- Coordinated the NSIE Multilateral Meeting, convening NSIE, government, and private sector representatives to focus on information sharing, issues surrounding advanced persistent threats, supply chain, and workplace cybersecurity technology management.
- Completed the National Security Telecommunications Advisory Committee *Report to the President on Communications Resiliency*, which addresses resilience, challenges, and mitigation activities under four disaster scenarios and discusses investments or actions that the Federal Government could take to enhance the resilience of communications services.
- Established the Cloud Computing Scoping Subcommittee to examine cloud computing data, infrastructure, resilience, interdependencies, and potential impacts on NS/EP communications.
- Initiated compliance assessments for Wireless Priority Service (WPS) and will begin similar assessments for the NCS Government Emergency Telecommunications Service (GETS) and Telecommunications Service Priority (TSP) programs.

"The President's National Security Telecommunications Advisory Committee (NSTAC) provided the President with new recommendations on communications resiliency and saw the implementation of previous recommendations from their Identity Management report manifested in the recently released National Strategy for Trusted Identities in Cyberspace (NSTIC)."

Source: 2011 Communications Sector Annual Report

"The Communications Sector is now focusing its risk assessments on communications architecture elements rather than specific assets, systems, and networks. In 2010, Homeland Infrastructure Threat and Risk Analysis Center's (HITRAC) methodology moved from attribute-based criteria to consequence-based criteria for its Level 1 and Level 2 asset program."

Source: 2011 Communications Sector Annual Report

- Established the Emerging Communications Technologies Forum to examine new and emerging technologies that could enhance NS/EP communications.
- Held a multiagency communications and cyber exercise through the cooperation of the Joint Telecommunications Resources Board and the Executive Office of the President related to national response authorities.
- Launched the 2011 NSRA to further reduce risk by examining threats to the communications infrastructure (e.g., Wireline, wireless, satellite, cable, and broadcast), inform risk management decisions to enhance the resilience of the communications landscape, and disclose findings to public and private decisionmakers and Federal, State, local, tribal, and territorial stakeholders.
- Held an Emergency Support Function (ESF) Spring Training and Exercise Workshop that featured lectures, onsite equipment tours, and a scenario-based exercise that simulated the response activities of State and local governments with the infusion of Federal and private sector resources, that were coordinated by the Federal interagency ESF #2 team members.

Key Initiatives

The Communications Sector continues to promote and improve partnerships that will help government and industry stakeholders prevent, prepare for, detect, mitigate, and respond to a major disruption of critical communications services. Current initiatives include:

- Developing mechanisms to support rapid reconstitution of critical communications services after national and regional emergencies, including cybersecurity emergencies.
- Working with industry to improve cross-sector coordination mechanisms and address critical interdependencies, including cybersecurity interdependencies.
- Strengthening continuity of government and operations capabilities across NS/EP users via NCS Directive 3-10, Minimum Requirements for Continuity Communications Capabilities, by participating and testing various continuity mechanisms in government exercises.
- Improving information-sharing programs for government and industry partners at the Federal, State, and local levels.
- Conducting joint exercises and training initiatives with government and industry partners to enhance critical infrastructure protection and response by participating in Cyber Storm III and Eagle Horizon.
- Assisting international partners to further develop and improve Network Security Information Exchanges to mitigate cyber intrusions in public telephone networks.
- Providing communications services to mitigate network congestion or disruption via priority services programs such as TSP, GETS, and WPS.
- Completing Phase I of the NSRA in fall 2011—an enhancement and update of the 2008 NSRA jointly written by government and industry partners.

"The [National Communications System] Standards Team works with a number of national and international industry standards organizations to ensure that evolving communications standards address the technical requirements of [national security/ emergency preparedness] communications."

Source: 2011 Communications Sector Annual Report

Path Forward

The Communications Sector will continue to conduct activities to secure its assets, systems, and networks. These activities include the following:

- Continue to support the development of Next Generation Networks priority services to meet the evolving requirements of critical communications customers in a converged communications environment.
- Collaborate with sector partners to better understand and effectively address the security concerns associated with the deployment of the proposed National Public Broadband Safety Network.
- 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.
- Promote educational programs on communications technologies and their potential points of failure during emergencies.
- Promote timely, relevant, and accurate threat information sharing between law enforcement, intelligence communities, and key decisionmakers in the sector with the appropriate industry partners.
- Continue to develop procedures to obtain stakeholder inputs for incorporation into the NSRA risk assessment updates.

GCC MEMBERS

- Federal Communications Commission
- Federal Reserve Board
- General Services Administration
- National Association of Regulatory Utility Commissioners
- Nuclear Regulatory Commission
- U.S. Coast Guard
- U.S. Department of Agriculture
- 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 the Interior
- U.S. Department of Justice
- U.S. Department of State

SCC MEMBERS

- 3U Technologies, LLC
- Alcatel-Lucent
- Americom-GS
- Association of Public Television Stations
- AT&T
- The Boeing Company
- Century Link
- CTIA - The Wireless Association
- Cincinnati Bell
- Cisco Systems, Inc.
- Comcast
- Computer Sciences Corporation
- Digi International
- DirecTV
- Harris Corporation

SCC MEMBERS CONTINUED

- Hughes Network Systems
- Internet Security Alliance
- Intrado
- Iridium
- Juniper Networks
- Level 3 Communications
- McLeodUSA
- The MITRE Corporation
- Motorola
- National Association of Broadcasters
- National Cable & Telecommunications Association
- NeuStar
- Nortel
- Powerwave
- Research in Motion
- Rural Cellular Association
- The Satellite Broadcasting and Communications Association
- Satellite Industry Association
- Savvis, Inc.
- Sprint
- Telcordia
- Telecommunications Industry Association
- TeleContinuity, Inc.
- TerreStar Networks, Inc.
- Tyco
- Utilities Telecom Council
- U.S. Internet Services Provider Association
- U.S. Telecom Association
- VeriSign Authentication Services
- 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. Products designed, produced, and distributed by U.S. manufacturers make up 13 percent of the U.S. gross domestic product and directly employ approximately 11.7 million of the Nation's workforce. The Critical Manufacturing Sector Coordinating Council (SCC) currently includes representatives from 47 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) National Protection and Programs Directorate's Office of Infrastructure Protection is the Sector-Specific Agency for the Critical Manufacturing Sector.

Vision

To reduce the 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 partnerships and a renewed focus on outcomes.

Goals

The following goals were developed in support of the sector's vision and help provide the basis for ongoing risk management activities:

- Achieve an understanding of the assets, systems, and networks that comprise the critical infrastructure of the Critical Manufacturing Sector.
- Develop an up-to-date risk profile of the assets, systems, and networks within the Critical Manufacturing Sector that will enable a risk-based prioritization of protection activities.
- Develop protective programs and 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 the Critical Manufacturing Sector's 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 undertaken measures over the past year to increase the sector's security and resilience posture, which include:

- Participated in the Regional Resiliency Assessment Program to analyze a region's clusters of infrastructure assets and their associated interdependencies.
- Briefed on the planning, preparation, and exercise of Cyber Storm III, an exercise that created a national-level incident in which critical infrastructure partners tested their facilities' cybersecurity plans, as well as individual company plans.
- Partnered with the Transportation Security Administration (TSA) Highway and Motor Carrier Division and the private sector to conduct six Supply Chain Security Exercises that included scenario elements such as natural disasters, information technology/cyber concerns, closed border crossings, and terrorist activities.
- Completed an After Action Report following the planning and execution of the Supply Chain Security Exercise, which included best practices, lessons learned, and recommendations for improvements to evaluate the effectiveness of each partner's ability to respond to and recover from major incidents.
- Conducted six Enhanced Critical Infrastructure Protection (ECIP) visits in the past year for the Critical Manufacturing Sector and plans to conduct 800 to 1,000 ECIP visits of all 18 Critical Infrastructure Sectors in the coming year.
- Created a more representative SCC by providing an outreach initiative tailored to regional small- and medium-sized manufacturers, resulting in 16 new sector members.
- Established the Critical Manufacturing Cybersecurity Working Group in January 2011 to share information from government authorities and subject matter experts and to provide a forum for industry partners to discuss cybersecurity issues.
- Hosted regular monthly Information Sharing Working Group meetings since September 2010 to provide sector members information based on membership-prioritized requests to ensure that effective and meaningful information is articulated within an established and collaborative information-sharing environment.
- Developed and co-founded the Cross-Sector Supply Chain Working Group to identify and share best practices for supply chain risk management between government and industry, as well as to help foster a working relationship between industries.

"Through the CM [Critical Manufacturing] Sector Security Conference, the CM [Sector-Specific Agency] strives to foster a collaborative communications process between CM Sector partners. The conference provides a venue for partners to meet, and a place to discuss industry-specific infrastructure security and resiliency issues with key government representatives. Furthermore, this security conference will aim to engage public and private sector collaboration by working to improve situational awareness and sharing appropriate threat and vulnerability information."

Source: 2011 Critical Manufacturing Sector Annual Report

"The GCC [Government Coordinating Council] continues to serve as a successful forum of collaboration among public entities that have a stake in securing the CM [Critical Manufacturing] Sector. The GCC meetings have proven to be an effective way for members to meet and discuss CM security issues across several Federal agencies and at the State and local government levels."

Source: 2011 Critical Manufacturing Sector Annual Report

- Hosted the inaugural Critical Manufacturing Partnership Road Show, which invited industry partners to participate in onsite visits to various DHS facilities and provided high-level classified and unclassified briefings to gather time-sensitive information and sector-specific intelligence.

Key Initiatives

Sector partners, both public and private, are engaging in a wide variety of activities to mitigate risks to critical infrastructure, including:

- Identifying and reviewing the critical assets of each of the Critical Manufacturing Sector's functional areas including human, physical, and cyber components that support the Nation's security, economy, public health, and safety.
- Assessing and prioritizing risks to the sector's functional areas, including evaluating emerging threats and vulnerabilities and mapping them to the infrastructure to prioritize protective efforts.
- Tailoring protective measures, which mitigate associated consequences, vulnerabilities, and threats, to accommodate the full diversity of the sector.
- Developing and sharing effective security practices and protective measures with critical infrastructure partners.
- Identifying and ensuring the availability of resources (pre- and post-incident) that are essential to the sector's effective recovery following an incident.
- Developing metrics for measuring the effectiveness of the sector's critical infrastructure protection efforts and developing a method to gather the needed information that is not unduly burdensome on asset owners and operators or other partners.
- Developing a means for reporting on critical infrastructure protection effectiveness to relevant partners throughout Federal, State, and local governments, as well as the private sector.
- Improving situational awareness during normal operations, developing situations, and actual incidents.
- Developing the first-ever Critical Manufacturing Sector Security Conference (held August 30–31, 2011) to aid manufacturing partners in efforts to manage and implement protection and continuity of operations planning and elevate awareness and understanding of threats and vulnerabilities to their assets, systems, and networks.
- Moving forward with plans to make the inaugural Critical Manufacturing Partnership Road Show (held in April 2011) an annual event which showcases the depth of resources available through DHS to benefit the private sector.
- Collaborating, developing, and sharing appropriate threat and vulnerability information among public and private sector partners, including development of indications and warnings.
- Developing and maintaining incident response and coordination plans and procedures.
- Participating in exercises for validating communication protocols, response plans, and procedures necessary to reduce recovery time following an incident.

"The SSA [Sector-Specific Agency] outreach strategy supports metrics development through the feedback mechanisms incorporated into the trainings, tools, and major information sharing programs. The SSA will continue to use these mechanisms to improve the quality and type of information shared, and use partner feedback to direct programs where they are needed and requested. The SSA will also research data requirements to develop new quantitative output and outcome metrics."

Source: 2011 Critical Manufacturing Sector Annual Report

Path Forward

To enhance the protection and resilience of its assets, the Critical Manufacturing Sector will:

- Build and maintain cybersecurity collaboration and engagement across the sector.
- Focus limited resources on the highest security risks in the current economic climate.
- Develop and collect metrics data with a focus on outcomes and risk reduction.
- Improve fusion center coordination and collaboration with DHS and the private sector.
- Partner with TSA, State homeland security advisors, State emergency managers, and others across the country to deliver Supply Chain Security Exercise Series and SSA-sponsored programs to industry stakeholders.
- Create and distribute a one-page document describing Critical Manufacturing SSA trainings, tools, and publications to raise awareness of the free, voluntary programs available to sector partners.
- Partner with the Infrastructure Security Compliance Division to leverage their resources to notify private sector partners when SSA-sponsored programs will be offered in their region, such as the Critical Manufacturing Regional Outreach effort.
- Coordinate with the Manufacturing Extension Partnership community to reach more than two dozen small- to mid-sized manufacturers and offer security resources such as business continuity training and planning.

GCC MEMBERS

- Small Business Administration
- 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 the Interior
- U.S. Department of Justice
- U.S. Department of Labor
- U.S. Department of State
- U.S. Department of Transportation
- U.S. Department of the Treasury
- U.S. Environmental Protection Agency

SCC MEMBERS

- Aerojet, a GenCorp Inc.
- Alexion Pharmaceuticals, Inc.
- ArcelorMittal USA
- The Boeing Company
- Bridgestone Americas, Inc.
- Carpenter Technology Corporation
- Caterpillar, Inc.
- Chrysler Group, LLC
- Cisco Systems, Inc.
- Crane Aerospace & Electronics
- Deere & Company
- Delbia Do Company
- Delphi Corporation
- Ellanef Manufacturing
- Emerson Electric, Co.
- Ford Motor Company
- General Electric Company
- General Motors Company

SCC MEMBERS CONTINUED

- Goodyear Tire & Rubber Company
- GrayGlass
- Hercules Heat Treating Corp.
- Intel Corporation
- ITT Corporation
- Johnson Controls, Inc.
- Kohler Company
- Lee Spring Co.
- Mi-Jack Systems & Technologies, LLC
- Mini-Circuits
- Navistar International Corporation
- Nichols Brothers Boat Builders
- Oshkosh Corporation
- PACCAR
- Pelco, by Schneider Electric
- Penske Corporation
- Raytheon Company
- Remy International, Inc.
- Rosco Vision Systems
- S&L Aerospace Metals, LLC
- Schweitzer Engineering Laboratories, Inc.
- Smith & Wesson Holding Company
- Steeler Inc.
- Summit Appliances, Inc.
- ThyssenKrupp Stainless Steel USA, LLC
- United Technologies Corporation
- U.S. Steel Corporation
- Whirlpool Corporation
- Zero International

DAMS SECTOR

Partnership

The Dams Sector comprises 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 Sector SCC is composed of non-Federal owners and operators as well as trade associations, and it 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 various levels of government (Federal, State, local, tribal, and territorial), including Federal owners and operators, and State and Federal regulators of sector assets. The Department of Homeland Security National Protection and Programs Directorate's Office of Infrastructure Protection serves as the Sector-Specific Agency and the GCC Chair for the Dams Sector.

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, multilevel, 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 partnerships 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. The sector's accomplishments over the past year include the following:

- Vetted applications and granted access for 185 new users of the Homeland Security Information Network-Critical Sectors (HSIN-CS) Dams Portal.
- Utilized the Dams Sector Suspicious Activity Reporting tool to report 81 occurrences of suspicious activity.
- Completed and released an online training course, Independent Study (IS)-872 *Dams Sector: Protective Measures*, which addresses protective measures related to physical, cyber, and human elements (445 users to date).
- Developed two technical reference documents: *Estimating Loss of Life for Dam Failure Scenarios* and *Estimating Economic Consequences for Dam Failure Scenarios.*
- Conducted the Third Annual National Dam Security Forum in conjunction with the Association of State Dam Safety Officials Dam Safety Conference held from September 19–23, 2010, in Seattle, WA.
- Conducted the 2010 Dams Sector Exercise Series – Green River Valley (Washington State), which focused on the analysis of short- and long-term regional impacts resulting from a flooding scenario affecting a large portion of the Green River Valley.

"The National Inventory of Dams (NID) lists over 82,000 dams; the total number of dams in the Nation, including those not included within the NID, is estimated at 100,000."

Source: 2011 Dams Sector Annual Report

"The Suspicious Activity Reporting tool is a key risk mitigation effort for the Dams Sector. Between May 10, 2010 and April 2011, 81 occurrences of suspicious activities were reported through the Suspicious Activity Reporting tool. Stakeholder reports of suspicious activity increased by 40 percent from the nine months of the previous year (the reporting system became operational in August 2009)."

Source: 2011 Dams Sector Annual Report

- Collaborated on the development of the Dam Security and Protection Technical Seminar.
- Developed the Dams Sector Analysis Tool to provide secure access to a series of Web-based modules and applications covering a wide range of analytical capabilities.
- Released the *Roadmap to Secure Control Systems in the Dams Sector.*

Key Initiatives

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

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

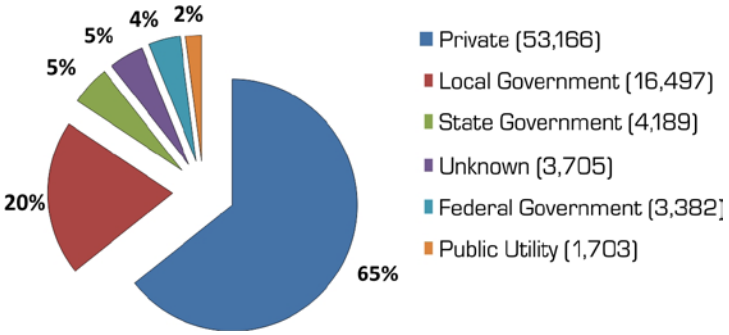
- Compile lessons learned from the challenges associated with implementing the existing cybersecurity regulatory standards.
- Continue to safeguard facility-sensitive information from disclosure.
- Continue to identify and characterize critical assets in an effort to demonstrate the need for a risk-based, multiyear, and multijurisdictional infrastructure rehabilitation program.
- Increase reliance on HSIN-CS by enabling virtual participation in sector quarterly councils and workgroup meetings.

"In the reporting year, the sector released an online training course, Independent Study (IS)-872 Dams Sector: Protective Measures, which addresses protective measures related to physical, cyber, and human elements. It describes the importance of these measures as components of an overall risk management program. The Web-based course describes the basic elements of risk management, discusses the steps required to develop and implement an effective protective program, and assists stakeholders in developing protective programs based on a systematic assessment of threats, selected level of protection, and consideration of constraints."

Source: 2011 Dams Sector Annual Report

Dams Ownership Structure

National Inventory of Dams-listed Assets



GCC MEMBERS

- Bonneville Power Administration
- Federal Energy Regulatory Commission
- State of California, Department of Water Resources
- State of Colorado, Division of Water Resources
- State of Nebraska, Department of Natural Resources
- State of New Jersey, Department of Environmental Protection
- State of North Carolina, Department of Environment and Natural Resources
- State of Ohio, Department of Natural Resources
- State of Pennsylvania, Department of Environmental Protection
- Tennessee Valley Authority
- U.S. Department of Agriculture
- 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 the Interior
- U.S. Department of Labor
- U.S. Department of State
- U.S. Environmental Protection Agency

SCC MEMBERS

- Allegheny Energy
- Ameren Services Company
- American Electric Power
- Association of State Dam Safety Officials
- Association of State Floodplain Managers
- Avista Utilities

SCC MEMBERS CONTINUED

- BC Hydro
- Chelan County
- Consumers Energy
- Colorado River Energy Distributors Association
- Dominion Resources
- Duke Energy Corporation
- Exelon Corporation
- Hydro-Québec
- National Association of Flood & Stormwater Management Agencies
- National Hydropower Association
- National Mining Association
- National Water Resources Association
- New York City Department of Environmental Protection
- New York Power Authority
- Ontario Power Generation
- Pacific Gas & Electric Company
- PPL Corporation
- Progress Energy
- Puget Sound Energy
- Salt River Project Water and Power
- SCANA Corporation
- Seattle City Light
- South Carolina Public Service Authority
- Southern California Edison
- Southern Company
- U.S. Society of Dams
- Xcel Energy Corporation

DEFENSE INDUSTRIAL BASE SECTOR

Partnership

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

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 critical infrastructure, or that by its nature would represent a high risk/high impact to critical infrastructure or DIB assets.

Selected Accomplishments

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

- Identified a potential gap in the process for determining the criticality of private sector DIB assets and responded by integrating defense industry experts into the annual criticality determination process.
- Developed a self-assessment tool for small- and medium-sized companies to use to assess physical security, cybersecurity, and resilience.
- Developed and deployed a private sector portal on the Homeland Security Information Network that allows sector owners and operators to access threat, warning, and risk information and enables participation in discussions, awareness Webinars, and other forms of collaboration.
- Implemented an emergency notification system that can reach sector SCC partners.

"The [Joint Business Plan] reenergized [U.S. Department of Defense] and private sector engagement within the national 14 CIKR protection framework and aided the DIB partnership to make concrete sector-wide progress."

Source: 2011 Defense Industrial Base Sector Annual Report

"To stimulate a broad range of government-industry information sharing, DOD is pursuing the national goal of a federated set of authoritative portals that allow industry stakeholders to visit one site for all of their information sharing needs."

Source: 2011 Defense Industrial Base Sector Annual Report

- Converted the DIB Cyber Security/Information Assurance Pilot to a program status.
- Formed the Defense Security Information Exchange that acts as a DIB SCC Cyber Security standing committee, and which the SCC formally designated as the Cyber Sub-Council in February 2008.

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:

- Participating in classified threat information-sharing roundtables.
- Planning two regional energy dependency assessments by the end of the Fiscal Year 2011 and recommending a dependency analysis methodology that partners may use.
- Identifying existing information-sharing portals and pursuing a system to host robust two-way classified information sharing.
- Working to improve sector information sharing at the local level and to integrate owners and operators into information-sharing environments at State and local fusion centers.

Path Forward

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

- Continue an increasingly partnership-oriented approach to refine, develop, and implement strategies and program implementation plans important to the protection and resilience of the sector.
- Pursue the active engagement of its SCC counterparts and all sector partners to refine existing processes and develop new processes required to eliminate unacceptable levels of risk.
- Revise the *Joint Business Plan for 2011–2012* to focus annual activity on a set of shared objectives, which will continue to be based on the goals of the Sector-Specific Plan and on current trends or threats that impact the sector.

"DOD recently approved $113 million for 2011–2016 to convert the DIB Cyber Security/Information Assurance Pilot to a program status."

Source: 2011 Defense Industrial Base Sector Annual Report

GCC MEMBERS

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

SCC MEMBERS

- AAI Corporation
- Aerojet, A GenCorp Inc.
- Aerospace Industries Association
- Alliant Techsystems
- American Society for Industrial Security International
- BAE Systems
- Ball Aerospace
- The Boeing Company
- Booz Allen Hamilton
- Computer Sciences Corporation
- Defense Security Information Exchange
- DRS Technologies, Inc.
- General Atomics
- General Dynamics
- General Electric Company
- Honeywell International
- Huntington Ingalls Industries
- Industrial Security Working Group
- L-3 Communications Corporation
- Lockheed Martin Corporation
- The MITRE Corporation
- National Classification Management Society
- National Defense Industrial Association
- Northrop Grumman Corporation
- Orbital Science Corporation
- Pratt & Whitney
- Raytheon Company
- Rockwell Collins
- Rolls-Royce North America
- Science Applications International Corporation
- SRA International, Inc.
- Textron, Inc.
- TASC Inc

EMERGENCY SERVICES SECTOR

Partnership

The Emergency Services Sector (ESS) is composed of prevention, protection, preparedness, response, and recovery elements that form the Nation's first line of defense for preventing and mitigating day-to-day incidents as well as catastrophic situations. 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 manmade), and aid recovery from emergency situations. In the ESS, owners and operators represent multiple distinct disciplines and systems that broadly reside within State and local government public safety agencies, but which also include private, for-profit businesses. The partnership activities and programs appropriate to the sector are those that maintain an inward-focused perspective and allow for the response community to remain able to engage in its mission during an all-hazards event.

The U.S. Department of Homeland Security (DHS) National Protection and Programs Directorate's Office of Infrastructure Protection (IP) serves as the Sector-Specific Agency (SSA) for the ESS. 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 coordinating critical infrastructure strategies, activities, policy, and communications within their organizations, across governments, and between government 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 six emergency service disciplines: law enforcement, fire and rescue, emergency medical services, emergency management, private security, 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 highlight 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 build an information-sharing environment that ensures the availability and flow of accurate, timely, and relevant information and intelligence about terrorist threats and other hazards, information analysis, and incident reporting.
- **Prevention, Preparedness, and Protection**: To employ a risk-based approach to developing protective efforts designed to improve the overall posture of the sector through targeted risk management decisions and initiatives.
- **Sustainability, Resilience, and Reconstitution**: To improve the sustainability and resilience of the sector and increase the speed and efficiency of restoring normal services, levels of security, and economic activity following an incident.

Selected Accomplishments

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

- Produced a working version of the Web-based Emergency Services Self-Assessment Tool (ESSAT).
- Developed a beta test of an exercise series that is specifically designed for first-responder managers.
- Achieved a 59 percent increase in the number of approved security clearances for SCC members and sector stakeholders sponsored by ESS.
- Distributed 1,000 First Responder Readiness Program informational packages through conferences and meetings.
- Registered 552 participants for the Ready Responder Program for the Emergency Services Sector Webinar and 140 participants for the Cybersecurity in the Emergency Services Sector Webinar.
- Developed the *Roadmap to Secure Voice and Data Systems in the Emergency Services Sector*, which is expected to be completed by the end of 2011.

"With support from [the U.S. Department of Homeland Security], leaders of the Nation's Emergency Services Sector have come together through the Emergency Services Sector Coordinating Council, to work together to protect and promote the Sector's capability to provide emergency services to the public and the Nation. Recent actions being taken by this Coordinating Council are aimed at providing significant new preparedness, response and recovery benefits for the Emergency Services Sector."

Source: John Thompson, Chair, Emergency Services Sector Coordinating Council

- Formed a broad-based Credentialing & Disaster Reentry Working Group to respond to the Nation's need for a standardized national approach to all-hazards/all-sectors crisis reentry that is coordinated across jurisdictional boundaries by public and private emergency responders.
- Formed a Pandemic Working Group that was expanded to a Working Group on Medical Countermeasures to respond to the lack of a national strategy for protecting the health of emergency services personnel, therefore protecting the capacity of the ESS.

Key Initiatives

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

- Establishing a Sector Initiatives Call to capture numerous activities impacting the ESS, which are communicated to the sector at regularly scheduled SCC and GCC meetings.
- Identifying and managing risk through DHS field facility security assessments, such as the Site Assistance Visits Program, the Buffer Zone Protection Program, and the Enhanced Critical Infrastructure Protection Program.
- Facilitating the improved sharing of timely, validated, protected, and actionable information supported by extensive education, training, and awareness programs through the ESS Information Sharing Working Group.
- Sharing up-to-date information by attending Critical Infrastructure Partnership Advisory Council conference calls, coordinating information calls with Federal partners responding to incidents, and posting unclassified but relevant information to the Homeland Security Information Network-Critical Sectors portal.
- Participating in the National Level Exercise 2011 and the Denver Interagency Continuity of Operations Exercise.
- Participating in the National Cyber Security Division's (NCSD) Cyber Exercise Program.
- Performing research and development for new technologies, such as mobile field biometrics; ambulance design standards; alerts and warnings using social media, personal alert, and tracking systems; and unified incident command and decision support.
- Developing a proposed path forward on crisis reentry and access control for public and private emergency responders nationwide by vetting and refining standards, processes, protocols, and best practices in credentialing and disaster reentry and seeking out approaches that are practical for nationwide adoption and implementation.

"The [Emergency Services Self-Assessment Tool] enables public and private entities to perform risk assessments of critical fixed assets and systems, on a local and regional level. The tool encourages voluntary and interactive stakeholder involvement and allows for a coordinated effort among sector partners by collecting and sharing common risk gaps, obstacles, and protective measures. The tool benefits individual partners and collective disciplines, and supports sector-wide risk management efforts."

Source: 2011 Emergency Services Sector Annual Report

Path Forward

To address future challenges, the sector will:

- Pilot the ESSAT at the New Jersey Office of Homeland Security and Preparedness, which will be the first State to pilot this tool, and then more than double the amount of assessments completed at ESS facilities per year by means of this tool.
- Continue to work collaboratively with NCSD throughout 2011 to assess the Cybersecurity Assessment and Risk Management Approach.
- Work to maintain personnel and personnel training, replace and repair existing and damaged equipment, and search for additional sources and resourceful methods to maintain and increase existing capabilities as grant money decreases and cities and municipalities address deep budget shortages.
- Continue to develop and implement sustainable risk management activities and develop outcome metrics.
- Promote cybersecurity activities and information sharing.
- Evaluate a Statewide Joint Standard Operating Procedure being implemented in Louisiana and the Mississippi Gulf Coast and a credentialing standard adopted by the National Sheriffs' Association (NSA), both developed with support from NSA, the Federal Bureau of Investigation's InfraGard Program, and others.
- Honor credentialing standards advanced by the DHS Science and Technology Directorate.
- Continue to build and maintain confidence among ESS personnel as to the effectiveness of planning for and responding to medical threats.

Emergency Services Sector Disciplines

- Law Enforcement
- Fire and Rescue Services
- Emergency Management
- Emergency Medical Services
- Private Security
- Public Works

GCC MEMBERS

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

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

SCC MEMBERS CONTINUED

- National Association of Security Companies
- National Association of State EMS Officials
- National Center for Emergency Preparedness at Vanderbilt University Medical Center
- National Emergency Management Association
- National Fire Protection Association
- National Native American Law Enforcement Association
- National Sheriffs' Association
- Rescobie Associates, Inc.
- Securitas Security Services
- Security Industry Association

ENERGY SECTOR

Partnership

The Energy Sector consists of thousands of geographically dispersed electricity, oil, and natural gas assets that are connected by systems and networks. Collaboration is essential to secure this interdependent infrastructure, which is owned, operated, hosted, and regulated by numerous public and private entities. The sector's public-private partnership allows sharing of information on threats, vulnerabilities, and protective measures. Private sector security partners are represented by two Sector Coordinating Councils (SCCs), the Electricity SCC and the Oil and Natural Gas SCC, which essentially represent all asset owners and operators. Public sector partners comprise the Energy Sector Government Coordinating Council (GCC). The U.S. Department of Energy serves as the Sector-Specific Agency (SSA) for 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 exchanges among trusted public and private sector security partners.
- Use sound risk management principles to implement physical and cyber measures that enhance preparedness, security, and resilience.
- Partner to conduct comprehensive emergency, disaster, and business continuity 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 those that may reach into other sectors and work to evaluate and address them by incorporating that knowledge into planning, training, exercises, and operations.
- Strengthen partner and public confidence in the sector's ability to manage risk by implementing effective security, reliability, and recovery efforts.

Selected Accomplishments

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

- Developed and approved sector-specific metrics survey questions for the Oil and Natural Gas Sector, which were aligned with the goals of the Transportation Security Administration pipeline modal SSA, and updated the *2011 Oil and Natural Gas Sector Coordinating Council (ONGSCC) Strategic Plan*.
- Released the *2011 ONGSCC Strategic Plan* and the *North American Electric Reliability Corporation (NERC) Electricity Critical Infrastructure Strategic Roadmap* in November 2010, which provides a framework to identify risks that have the potential to seriously disrupt the supply of electricity to customers and promotes the actions necessary to enhance the Electricity Sub-sector reliability and resilience.
- Developed the Electricity Subsector performance metrics aimed to inform, increase transparency, and quantify the effectiveness of risk reduction and mitigation actions, illustrating NERC reliability performance results and trends.
- Created the *Critical Infrastructure Protection Strategic Initiatives Coordination Action Plan*, in which NERC identifies four severe impact scenarios as an approach to address high-impact, low-frequency events with well-defined, strategic initiatives and priority recommendations.
- Released the revised Energy GCC Charter, with goals and responsibilities.
- Established the National Electric Sector Cybersecurity Organization.

"The BP Deepwater Horizon drilling rig explosion was considered one of the worst industrial accidents in history; fire engulfed and ultimately destroyed the rig, and oil was released into the Gulf of Mexico. The incident resulted in 11 crew-member deaths and other serious injuries, as well as enormous, continuing environmental and economic damage. The incident highlighted the potential for threats to stem from unexpected mechanical failure, and it served as a reminder of the importance of preparedness and risk mitigation. More importantly, this event demonstrated the difficulty of profiling all potential threats in a rapidly changing, all-hazards risk environment, as well as of accurately quantifying the consequences of these risks."

Source: 2011 Energy Sector Annual Report

"In spring 2011, four Northeastern States, New York, New Jersey, Connecticut, and Pennsylvania, developed the Regional Infrastructure Protection Plan (RIPP). Focusing on the electrical sector, the all-hazards RIPP workshop explored how damage to the regional network could affect other critical infrastructure sectors. This was a major public-private partnership effort, which involved focused cooperation from sector partners, including major electrical utilities in the region, [the National Electric Reliability Corporation], the Independent System Operators (ISOs), and several transformer manufacturers."

Source: 2011 Energy Sector Annual Report

- Reorganized the Electricity SCC to include five industry chief executive officers (CEOs), the President and CEO of NERC, and the Chair of NERC's Critical Infrastructure Protection Committee.

Key Initiatives

The Energy Sector is continuing the implementation of the following protective programs, which range from participating in cybersecurity and Smart Grid initiatives to studying the importance of hydroelectric power generation to the national economy and overall energy reliability:

- Conducting the first annual Grid Security Exercise in November 2011 involving more than 250 participants, which will test NERC's and the electricity industry's crisis response plans and validate current readiness in response to a cyber incident.
- Hosting the 2011 Grid Security Conference in October, part of NERC's ongoing security awareness program, designed to bring together industry and government security professionals to discuss grid cybersecurity concerns, trends, and best practices in security throughout the industry.
- Participating in a U.S. Department of Homeland Security (DHS) pilot program to better understand the intelligence needs of critical infrastructure owners and operators.
- Developing and transferring risk assessment methodologies, such as the Enhanced Critical Infrastructure Protection Initiative, which help identify vulnerabilities and enhance security through collaboration with Federal, State, local, and private sector stakeholders at critical sites.
- Finalizing the update to the *Roadmap to Secure Control Systems in the Energy Sector* and other strategic plans.
- Making significant progress in developing sector-specific metrics in the Electricity Subsector and the Oil and Natural Gas Subsector.
- Meeting regularly with DHS and other agencies to share approaches and implement security practices related to energy system reliability, survivability, and resilience.

Path Forward

Although significant progress has been made in securing the energy infrastructure, challenges remain, including addressing cyber vulnerabilities and managing the diversity and interdependencies of energy infrastructure across sectors and national boundaries. The Energy Sector will take the following steps to move forward:

- Build and strengthen existing critical infrastructure protection partnerships.
- Continue to work with other agencies and sectors to understand interdependencies and plan for contingencies.
- Reach out to the Nation's international energy partners to strengthen lines of communication, promote best practices, and share valuable lessons learned.
- Address cybersecurity vulnerabilities in the Energy Sector.
- Facilitate communication and information exchange through the Homeland Security Information Network; NERC's Electricity Sector Information Sharing and Analysis Center, the Office of Infrastructure Security and Energy Restoration's secure Web site, ISERnet; training and exercises; energy situation reports; and the *National Electric Sector Cybersecurity Organization Resource.*

"In early February 2011, a major winter storm hit Texas and delivered frigid temperatures, snow and ice that caused power outages and shut down power generators which resulted in rotating blackouts. Over 150 electric generation plants around the state went down and natural gas supplies were also affected. The storm hit just days before the Super Bowl which was held at the Dallas Cowboys stadium. As part of the Energy Assurance Planning Initiative, the State of Texas was better prepared to respond to these events as a result of planning and exercises."

Source: 2011 Energy Sector Annual Report

GCC MEMBERS

- Federal Energy Regulatory Commission
- National Association of Regulatory Utility Commissioners
- National Association of State Energy Officials
- National Governors Association
- National Resources Canada
- 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 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 Transportation
- U.S. Department of the Treasury
- U.S. Environmental Protection Agency

ELECTRICITY SCC MEMBERS

- American Transmission Company
- Independent Electricity System Operator, Ontario, Canada
- National Rural Electric Cooperative Association
- North American Electric Reliability Corporation
- Orlando Utilities Commission
- Sho-Me Power Electric Cooperative
- UIL Holdings Corporation

OIL AND NATURAL GAS SCC MEMBERS

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

ASSOCIATE SCC MEMBER TRADE ASSOCIATIONS

- Canadian Association of Petroleum Producers
- Canadian Energy Pipeline Association

FOOD AND AGRICULTURE SECTOR

Partnership

The Food and Agriculture (FA) Sector is composed of complex production, processing, and delivery systems that have the capacity to feed people within and beyond the Nation's boundaries. These food and agriculture systems, which are almost entirely under private ownership, operate in highly competitive global markets, strive to operate in harmony with the environment, and provide economic opportunities and improved quality of life for rural and urban citizens of the United States and others worldwide.

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, local, tribal, and territorial representatives from agricultural, public health, food, law enforcement, and other relevant government entities. The Sector-Specific Agencies (SSAs) for the FA Sector are the U.S. Department of Agriculture (USDA) and the U.S. Department of Health and Human Services Food and Drug Administration (FDA). USDA is responsible for production agriculture and food, which includes meat; poultry; and frozen, liquid, and dried egg products. FDA is responsible for all other food products. The SSAs have been assigned responsibility for overseeing and coordinating protection and resilience efforts for the FA Sector.

Vision

The FA 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 at separate enterprises.
- Expand laboratory systems and qualified personnel.

Selected Accomplishments

Sector accomplishments over the past year include the following:

- Developed value propositions for the FA Sector GCC and SCC and began strategic planning efforts for each council.
- Brought together 230 attendees to discuss issues, challenges, and proposed solutions for improving critical infrastructure protection and resilience at the Symposium on Food and Agriculture Security.
- Added FA Sector assets, systems, and clusters for 30 States as part of the 2011 National Critical Infrastructure Prioritization Program Data Call.
- Completed the *Fifth Annual Food Defense Plan Survey*, which found that 74 percent of establishments that are regulated by the USDA's Food Safety and Inspection Service have a functional food defense plan, well exceeding the Fiscal Year 2010 goal of 67 percent.
- Launched tools to help owners and operators identify mitigation strategies and preventive measures.
- Increased the number of Strengthening Community Agrosecurity Planning workshops to 19, covering 16 States.
- Continued to expand capability and capacity through proficiency testing for chemical and microbiological contaminants and demonstrated all-hazards response capability through activation in response to the Deepwater Horizon oil spill.
- Launched a beta version of the Food and Agriculture Readiness Measurement Toolkit for Federal partners in January 2011, and State, local, tribal, and territorial partners in April 2011.

Key Initiatives

Key initiatives within the FA Sector include:

- Improving awareness and visibility of the sector through strategic planning efforts.
- Developing a three-year exercise and training calendar.
- Refining and enhancing information sharing, collaboration, and communications processes that include regular newsletters and use of the Homeland Security Information Network-Food and Agriculture and FoodSHIELD.
- Continuing and expanding use of the Food and Agriculture Sector Criticality Assessment Tool.

"The [Food and Agriculture] Sector is composed of complex production, processing, and delivery systems and encompasses upwards of four million assets, including some two million farms, 900,000+ restaurants, 100,000+ food retail establishments, more than 166,000 registered domestic food manufacturing, processing, and holding facilities (including storage tanks and grain elevators) and approximately 252,400 registered foreign facilities."

Source: 2011 Food and Agriculture Sector Annual Report

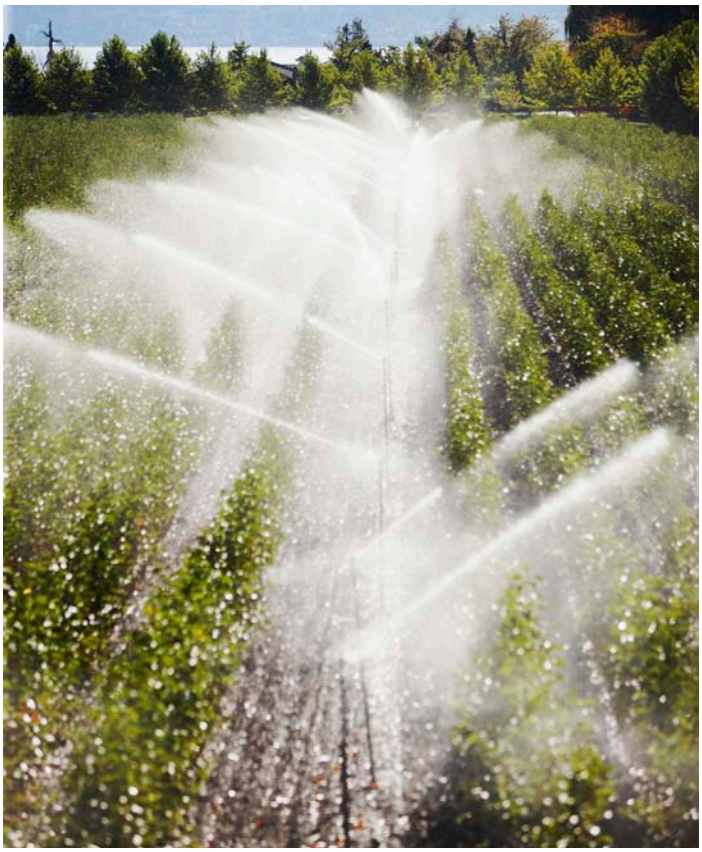
"On July 27, 2010, [the U.S. Department of Homeland Security Office of Infrastructure Protection] conducted a Food Service Food Defense Information Sharing Tabletop Exercise in conjunction with the FA Sector. The discussion-based, scenario-driven [tabletop exercise] was designed to allow exercise participants to focus on key information-sharing and response capabilities through a facilitated discussion."

Source: 2011 Food and Agriculture Sector Annual Report

Path Forward

To improve protection of the FA Sector, SSAs and sector partners are moving forward on many key actions. The FA Sector has an active GCC and SCC that coordinate protection activities. In 2010, both councils developed value proposition statements to improve awareness and engagement on FA Sector issues. These efforts will continue and form the foundation for broader strategic planning initiatives. The FA Sector will take numerous additional steps to move forward, including:

- Provide guidance to State, local, tribal, and territorial governments on leveraging Federal grant programs and related resources.
- Continue to meet on a regular basis to evaluate mechanisms and protocols for information sharing.
- Expand and leverage existing vulnerability and site assessment tools; in some cases, new assessment tools or modules may be required to address the unique aspects of the FA Sector, focusing on systems-based assessments.
- Identify tangible metrics to track and report sector progress on key risk mitigation activities.
- Work with the U.S. Department of Homeland Security to improve sector understanding of specific threats and promote broader collaboration on the assessment of cross-sector interdependencies.



"The [Food and Agriculture] Sector has designated [Homeland Security Information Network – Food and Agriculture] and FoodSHIELD as the two information-sharing platforms supporting the public and private sector."

Source: 2011 Food and Agriculture Sector Annual Report

GCC MEMBERS

- American Association of Veterinary Laboratory Diagnosticians
- Association of Food and Drug Officials
- Association of Public Health Laboratories
- Association of State and Territorial Health Officials
- Multi-State Partnership for Security in Agriculture
- 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
- The National Plant Board
- The Navajo Nation
- Southern Agriculture & Animal Disaster Response Alliance
- 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

SCC MEMBERS

- American Bakers Association
- American Farm Bureau Federation
- American Feed Industry Association
- American Frozen Food Institute
- American Meat Institute
- American Veterinary Medical Association
- Archer Daniels Midland Corporation
- Association of Food Industries
- Bob Evans Farms
- Cargill
- CF Industries, Inc.
- The Coca-Cola Company
- ConAgra Foods, Inc.
- Consumer Specialty Products Association
- Council for Responsible Nutrition
- CropLife America
- Dairy Institute of California
- Dean Foods Company
- Food Marketing Institute
- General Mills

SCC MEMBERS CONTINUED

- Giant Food, LLC
- Grocery Manufacturers Association
- H.J. Heinz Company
- International Association of Refrigerated Warehouses
- International Bottled Water Association
- International Dairy Foods Association
- International Flight Services Association
- International Food Service Distributors Association
- International Warehouse Logistics Association
- Juice Products Association
- Kellogg Company
- Keystone Foods
- Kraft Foods Global, Inc.
- The Kroger Company
- Marriott International
- McCormick & Company, Inc.
- Milkco, Inc.
- MillerCoors
- National Association of Convenience Stores
- National Cattlemen's Beef Association
- National Chicken Council
- National Confectioners Association
- National Corn Growers Association
- National Cotton Council of America
- National Fisheries Institute
- National Food Service Security Council
- National Grain and Feed Association
- National Grocers 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
- SES, Inc.
- Snack Food Association
- The Sugar Association
- Super Store Industry/Turlock Dairy Division
- 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 in the United States 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, the Federal Protective Service (FPS) is assigned as the Sector-Specific Agency responsible for the GFS. The Government Coordinating Council (GCC), chaired by FPS, is the primary coordination point and has representatives from government entities with responsibility for the protection of government facilities.

The GFS also includes the Education Facilities Subsector, which consists of all public and private schools, prekindergarten through 12th grade; and public and private higher education, 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:

- Reviewed and updated key risk mitigation activities.
- Leveraged its partnership model to implement plans that develop or expand processes to advance the identification of sector critical infrastructure assets, systems, and networks.
- Continued monthly Suspicious Activity conference calls for the benefit of GCC members.
- Identified a set of proxy activities that are representative of the sector at large.
- Participated in an internal measurement program to establish process improvement programs.

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 planning. Key initiatives within the sector include:

- Promoting awareness of and compliance with National Institute of Standards and Technology Special Publication 800-53: *Security Controls for Information Assurance.*
- Determining whether Federal facilities are in compliance with a range of physical security standards, including the Interagency Security Committee's Physical Security Criteria for Federal Facilities, through countermeasure effectiveness evaluation.
- Identifying Mission Essential Functions and Primary Mission Essential Functions to implement Federal Continuity Directives.
- Implementing and maintaining best-in-class security and protection support services at MegaCenters.
- Implementing the Office of Personnel Management's Electronic Questionnaires for Investigations Processing background investigation.
- Maintaining and/or revising Occupant Emergency Plans.

"The Government Facilities Sector (GFS) is one of the largest and most diverse sectors within the National Infrastructure Protection Plan (NIPP)."

Source: 2011 Government Facilities Sector Annual Report

"The sector is increasing attention to cybersecurity as its protective role expands from a human- and asset-centric philosophy to mission-continuity philosophy."

Source: 2011 Government Facilities Sector Annual Report

- Sustaining public safety through the Crime Prevention and Awareness program.
- Completing Facility Security Assessments in a timely and thorough fashion.
- Monitoring and promoting the implementation of key Federal information security initiatives.

Path Forward

Numerous steps will be taken as GFS addresses challenges to its success. These steps include the following:

- Enhance information technology (IT) systems and related operations to include systems and technologies for MegaCenters, the Risk Assessment and Management Program, 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.

"The GFS has continued many already established education, training, and outreach activities in the past year and initiated some new efforts."

Source: 2011 Government Facilities Sector Annual Report

GCC MEMBERS

- Architect of the Capitol
- City of Fort Worth, Texas
- City of Las Vegas, Nevada
- Clark County Office of Emergency Management
- General Services Administration
- National Academy of Sciences
- National Air and Space Administration
- National Archives and Records Administration
- Office of Personnel Management
- The Port Authority of New York and New Jersey
- Smithsonian Institution
- Social Security Administration
- State of New York, Division of Homeland Security and Emergency Management
- 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 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 Labor
- U.S. Department of State
- U.S. Department of Transportation
- U.S. Department of the Treasury
- U.S. Department of Veterans Affairs
- U.S. Environmental Protection Agency
- Wisconsin Department of Transportation

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 the Nation'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 its public sector members form the Government Coordinating Council (GCC). The U.S. Department of Health and Human Services (HHS) serves as the Sector-Specific Agency 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, such as water and 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. Sector accomplishments over the past year include the following:

- Prepared to implement a new asset identification process called the Critical Asset Identification Process, which enables the breakdown of the sector into a list of recommended Health Critical Assets, based on the asset nomination lists provided by the SCC subcouncil leadership; SCC subcouncils; and participating asset owners, operators, and sector subject matter experts (SME).
- Implemented quarterly classified briefings that are prepared and delivered in collaboration with the HHS Office of Security and Strategic Information and the U.S. Department of Homeland Security Homeland Infrastructure Threat and Risk Analysis Center.
- Increased the combined membership of the Homeland Security Information Network (HSIN) by roughly 30 percent over the course of the 2011 reporting period, enabling the sector to provide threat and risk information to hundreds more sector stakeholders.
- Developed a number of joint working groups to develop new ideas and products that provide specific benefits to the sector.
- Initiated the development of a cybersecurity primer document; a Water Sector subgroup brochure on best practices for water usage during a service interruption to HPH Sector facilities; and informational fact sheets outlining each working group's mission, goals, and objectives to recruit new SME membership.

Key Initiatives

The HPH Sector conducts numerous activities to improve its ability to maintain service continuity and mitigate risks to its workforce, physical assets, and cyber systems. Key initiatives within the sector include:

- Conducting unclassified briefings based on redacted information with larger audiences and giving presentations at various sector conferences to inform attendees about the critical infrastructure protection (CIP) program and a variety of CIP-related topics.
- Funding clearances for State health officials, public health leaders, and operational responders.

"On May 31 [the U.S. Department of Health and Human Services], in coordination with the Louisiana Department of Health and Hospitals, set up a mobile medical unit in Venice, Louisiana to provide triage and basic care for responders and residents concerned about health effects of the oil spill. The goal of this medical unit was to screen workers and citizens for exposure and refer those who require further care to local health care providers or hospitals. The goal was to support the local community and fill in any gaps that may be there, not to displace local providers."

Source: 2011 Healthcare and Public Health Sector Annual Report

- Disseminating a biweekly newsletter to all users highlighting HPH and CIP-focused articles and reports added to the HSIN-HPH portal document library, as well as a bimonthly newsletter providing updates on the initiatives and activities of the various sector working groups.
- Working with drug manufacturers, biological product manufacturers, and medical device manufacturers through the Drug, Biological Product, and Medical Device Shortage Programs of the U.S. Food and Drug Administration to plan for and manage potential or actual shortages that could have a significant impact on public health.
- Developing an approach to assess risks and defining a path forward to continue improving the process.

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:

- Work to increase participation from partners at all levels of government and the private sector to expand information-sharing efforts and establish a collaborative environment for sector partners to improve risk mitigation and information-sharing activities.
- Focus the Critical Asset Identification Process scenario development on threats that the intelligence community indicates have a realistic chance of impacting the sector.

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

- 3M
- Abbott Laboratories
- AdvaMed
- Aetna, Inc.
- Alexion Pharmaceuticals, Inc.
- American Academy of Nurse Practitioners
- American Academy of Pediatrics
- American Academy of Physicians Assistants
- American Association of Blood Banks
- American Association of Colleges of Pharmacy
- American Association of Tissue Banks
- American College of Emergency Physicians

"In response to the post-earthquake Cholera outbreak in Haiti, [the U.S. Department of Health and Human Services] deployed over 1,100 personnel to Haiti. This included [the Center for Disease Control's] public health experts, doctors, and nurses who staffed the twelve disaster medical assistance teams that were sent to Haiti and the disaster mortuary team working to help recover those who lost their lives in the quake. They have been supported by thousands of other staff in the United States."

Source: 2011 Healthcare and Public Health Sector Annual Report

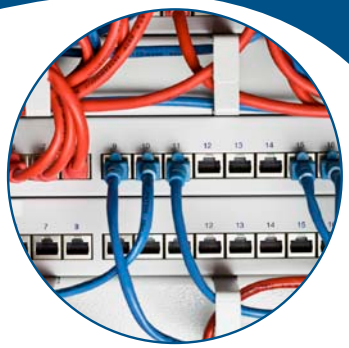
SCC MEMBERS CONTINUED

- American College of Occupational and Environmental Medicine
- American College of Physicians
- American Healthcare Association
- American Hospital Association
- American Industrial Hygiene 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.
- Archdiocese of Washington
- Association of Healthcare Resource and Materials Management Professionals
- Baxter Healthcare Corporation
- Baylor Health Care System
- Biotechnology Industry Organization
- Blood Centers of America
- Blue Cross and Blue Shield of Florida
- Blue Shield of California
- BLU-MED Response Systems
- Business Continuity Consulting
- Cardinal Health
- Casket and Funeral Supply Association
- Catholic Cemetery Conference
- Control Risks
- Cremation Association of North America
- Dartmouth Hitchcock Medical Center
- Dodge Company
- Generic Pharmaceutical Association
- The George Washington University Medical Center
- Greater New York Hospital Association
- Group Health Cooperative
- Hanover Hospital
- Health Industry Distributors Association
- Health Promotion Consultants
- Healthcare Distribution Management Association
- Healthcare Information and Management Systems Society
- Henry Schein, Inc.
- Hospital Association of Southern California
- Humana
- Independence Blue Cross
- Integrated Business Systems & Services, Inc.
- International Association for Healthcare Security & Safety
- International Cemetery, Cremation, and Funeral Association

SCC MEMBERS CONTINUED

- James B. Haggin Memorial Hospital
- Johns Hopkins University
- Johnson Memorial Medical Center
- The Joint Commission
- Kaiser Permanente
- Laboratory Corporation
- Lafayette General Medical Center
- Matthews Cremation
- Medco Health Solutions, Inc.
- Medline Industries, Inc.
- Memorial Sloan Kettering Cancer Center
- Merck & Co., Inc.
- Monmouth Ocean Hospital Service Corporation
- Mount Sinai & Schwab Rehabilitation Hospitals
- MVP Health Care
- National Association of Chain Drug Stores
- National Association of Nuclear Pharmacies
- National Association of Psychiatric Health Systems
- National Community Pharmacists Association
- National Council of State Boards of Nursing
- National Funeral Directors Association
- National Funeral Directors and Morticians Association
- National Health Information Sharing & Analysis Center
- Nemours
- Nevada Hospital Association
- Operation PAR, Inc.
- Owens & Minor, Inc.
- Pharmaceutical Research and Manufacturers of America
- Samaritan Health Services
- Siemens Healthcare USA
- SMA Technology Group
- Terumo Medical Corporation
- Texas A&M University
- Tuomey Healthcare System
- UCLA Medical Center Occupational Health Facility
- Universal Hospital Services
- University of Montana
- Verizon Business
- Virginia Hospital & Healthcare Association
- The Walt Disney Company
- Washington Occupational Health Associates, Inc.
- WellPoint, Inc.

INFORMATION TECHNOLOGY SECTOR



Partnership

The 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 U.S. 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 for a secure, resilient infrastructure, leveraging risk management and innovation to proactively prevent and protect against incidents and minimize the impact of the incidents that do occur to the sector and those dependent on critical IT Sector 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. Sector accomplishments over the past year include the following:

- Shared information, priorities, and experiences through monthly and ad hoc implementation working groups.
- Developed strategies to manage risks that were identified in the baseline IT Sector Risk Assessment (ITSRA) for IT products and services; incident management capabilities; domain name resolution services; and Internet routing, access, and connection services.
- Assessed additional IT Sector risks, including identity management, and performed an associated trust support services risk assessment as well as dependencies analysis.
- Examined and identified areas for improvement in incident response policy and operations by contributing to and participating in the Cyber Storm III exercise, which simulated national-level cybersecurity incidents.
- Helped establish a strategic framework for organizational roles; responsibilities; and actions to prepare for, respond to, and coordinate recovery from a cyber incident by contributing to the development of the National Cyber Incident Response Plan.

"The high degree of the IT Sector's interdependency and interconnectedness, and the easy anonymity of actors, makes identifying threats, assessing vulnerabilities, and estimating consequence difficult."

Source: 2011 Information Technology Sector Annual Report

"With the completion of the baseline [IT Sector Risk Assessment] and the risks and areas for future study identified in it, the IT Sector has developed a foundation from which it can conduct not only future risk assessments but also engage security partners in the development of risk management strategies."

Source: 2011 Information Technology Sector Annual Report

Key Initiatives

Key initiatives within the IT Sector include:

- Promoting response and recovery by coordinating with DHS and other sectors on cyber incidents.
- 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 as well as cybersecurity outreach and awareness.
- Providing leadership for cross-sector cybersecurity through the CSCSWG and other information-sharing and protective security programs, including US-CERT.
- Providing proper and consistent security training and education at both the national and organizational levels about the importance and impact of cybersecurity.
- Developing, implementing, and promulgating supply chain risk management practices through multiple forums (e.g., the National Institute of Standards and Technology, OpenGroup Trusted Technology Forum, and International Organization for Standardization).

Path Forward

The baseline ITSRA and the subsequent IT Sector Risk Management (ITSRM) strategies are the result of unprecedented partnership among government and industry entities that engaged in a collaborative and iterative process to assess and manage risk to six of the critical IT Sector functions. Throughout 2011 and 2012, IT Sector partners will take the following steps to build on the success of the baseline ITSRA and the ITSRM strategies:

- Foster implementation of identified risk management strategies by public and private sector partners.
- Continue to advance and improve information sharing and situational awareness to promote a comprehensive approach to national-level incident detection and response.
- Develop and participate in exercises, as appropriate, to identify areas for improvement and needed capabilities across the IT Sector.
- Perform additional risk analyses, as needed, on areas of concern to the IT Sector.

"Members of the IT Sector were also key participants in the development of the National Cyber Incident Response Plan (NCIRP). The NCIRP sets the strategic direction for how the Nation responds to everyday cyber incidents and how these steady-state operations are escalated into nationally coordinated response activities."

Source: 2011 Information Technology Sector Annual Report

GCC MEMBERS

- General Services Administration
- National Association of State Chief Information Officers
- Office of the Director of National Intelligence
- 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.
- Adobe Systems Incorporated
- Advanced Micro Devices
- Afilias USA, Inc.
- Arxan Defense Systems, Inc. & Dunrath Capital
- Bell Security Solutions Inc.
- Bivio Networks
- Business Software Alliance
- Center for Internet Security
- Certichron Inc
- Cisco Systems, Inc.
- Coal Fire Systems
- Computer and Communications Industry Association
- Computer Associates International
- Computer Sciences Corporation
- Core Security Technologies
- Cyber Pack Ventures Inc.
- Cyber Security Industry Alliance
- Computing Technology Industry Association
- Concert Technologies
- Dell
- Deloitte & Touche LLP
- Detica
- Dynetics, Inc.
- Ebay
- Echelon One
- Electronic Industries Alliance
- EMC Corporation
- Entrust, Inc.
- Equifax, Inc.
- EWA Information & Infrastructure Technologies, Inc.
- General Atomics
- General Dynamics
- Green Hills Software
- Google
- Hatha Systems
- Hewlett-Packard
- IBM Corporation
- Information Systems Security Association

SCC MEMBERS CONTINUED

- Intel Corporation
- Information Technology Industry Council
- Information Technology - Information Sharing & Analysis Center
- International Systems Security Engineering Association
- Internet Security Alliance
- International Security Trust and Privacy Alliance
- ITT Corporation
- Juniper Networks
- KPMG LLP
- L-3 Communications
- Lancope, Inc
- Litmus Logic
- LGS Innovations
- Lockheed Martin
- Lumeta Corporation
- Lunar Line
- Microsoft Corporation
- NetStar-1
- Neustar
- Northrop Grumman
- NTT America
- One Consulting Group
- One Enterprise Consulting Group, LLC
- Pragmatics
- R & H Security Consulting LLC
- Rackspace Hosting
- Raytheon
- Reclamere
- Renesys Corporation
- Research in Motion
- SAFE-BioPharma
- SafeNet Government Solutions
- Seagate Technology
- SecureState
- Sentar Inc
- The SI Organization
- Siemens Healthcare
- Serco
- Sun Microsystems, Inc.
- Symantec Corporation
- System 1
- TASC Incorporated
- Team Cymru
- TechAmerica
- Telecontinuity, Inc.
- Terremark World Wide
- TestPros, Inc.
- Triumfant
- Tyco
- 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 U.S. Government. However, based on the primary uses of some physical structures considered monuments or icons (e.g., the Golden Gate Bridge, the 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 and therefore does not host a Sector Coordinating Council, though it has partnered with the Government Facilities Sector to coordinate outreach to the various State, local, tribal, territorial, and private sector 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 the 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 cross-sector coordination with 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.
- 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. The sector's accomplishments over the past year include the following:

- Conducted security assessments at six sector assets and encouraged sector partners to perform independent assessments and update protective systems.
- Worked extensively with U.S. Department of Homeland Security National Cyber Security Division to begin assessments.
- Partnered with the Government Facilities Sector to coordinate outreach to State, local, tribal, territorial, and private sector entities.
- Shared training opportunities, protective best practices, and intelligence reporting through established portals.
- Identified issues that require government coordination and communication, as well as needs and gaps in plans, programs, policies, procedures, and strategies.
- Installed a camera system at the Mount Rushmore National Memorial and additional shipping and receiving screening points at the Jefferson National Expansion Memorial.
- Replaced explosive trace-detection units and magnetometers at the Washington Monument.
- Provided funds to the city of Philadelphia to improve camera coverage and surveillance ability throughout the city and its parks.
- Provided funding for the maintenance of the National Mall cameras.
- Made progress in construction of hardened security barriers at multiple national museums.

"Significant progress has been made within the NMI Sector post-9/11. In many cases, GCC sector partners had appropriated funds specifically targeted to protection, resulting in a more robust security posture at NMI Sector assets. The NMI Sector now faces the challenges of maintaining this level of security, continuing to justify the need for additional funding for improvements, and developing strategies and protective measures to deal with emerging threats."

Source: 2011 National Monuments and Icons Sector Annual Report

- Completed the addition of 247 proximity card readers to provide protection of National Archives and Records Administration (NARA) holdings and implemented a new program to screen personnel exiting the employee/research side of the NARA facility to prevent loss of holdings.
- Continued the Community Anti-terrorism Training "Cat Eyes" initiative in an effort to use maintenance, interpretive, and concessions staff and other employees to serve as eyes and ears for any suspicious activity surrounding sector assets.

Key Initiatives

The NMI Sector is implementing a variety of protective programs, which include protective system assessments and the sharing of training opportunities, protective best practices, and intelligence reporting through established portals. Together, these programs have contributed to a more secure and resilient sector. Key initiatives within the sector include:

- Funding additional commissioned law enforcement and contract security personnel positions to sustain 360-degree security coverage and to maintain staffing for other mission requirements.
- Developing unobtrusive physical security techniques and/or environmental/architectural designs that enhance perimeter security; cost-effective visitor screening technology that maintains accessibility and/or unobtrusive surveillance; and reliable chemical, biological, radiological, nuclear, and explosive detection systems.
- Supporting workforce surety through the implementation of a standard identity credential for secure and reliable identification and authentication of Federal Government employees and contractors.
- Implementing civil aviation restrictions around critical infrastructure assets located outside of the Washington, D.C., metropolitan area.
- Participating in the Buffer Zone Protection Program development and other security-related initiatives, such as the Lower Manhattan Protection Zone.
- Promoting the use of the Homeland Security Information Network-Critical Sectors secure portal by GCC partners as a practical means of sharing information concerning physical and cyber threats, vulnerabilities, incidents, potential protective measures, and effective security practices.

Path Forward

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

- Upgrade and improve the affordability of technologies for maintaining a controlled perimeter; visitor screening, surveillance, and interdiction; internal and external security; suspicious behavior studies and monitoring; and damage prediction capabilities.
- Monitor active research projects that develop physical security technologies, architecture that enhances security through environmental design, and other innovative means to protect sector assets.
- Conduct projects to replace or install surveillance radar, the park key system, the public address system, closed circuit television systems, vehicle bollards, X-ray screening equipment, magnetometers, explosive trace detection equipment, electronic security and access control perimeter security barriers, and blast protection at various sector assets as funding becomes available.

"NMI has established an individual account on the [Homeland Security Information Network – Critical Sectors] portal. Since the implementation, security partners have been nominated, adjudicated and activated their accounts. Training was held, Webinars were presented, and [the] end result was better access to vital critical sector information."

Source: 2011 National Monuments and Icons Sector Annual Report

GCC MEMBERS

- National Archives and Records Administration
- Smithsonian Institution
- U.S. Capitol Police
- U.S. Department of Homeland Security
- U.S. Department of the Interior
- U.S. Department of Justice

NUCLEAR SECTOR

Partnership

The Nuclear Sector includes the Nation's 65 commercial nuclear power plants, which provide approximately 20 percent of the electricity used in the United States. The sector also includes non-power reactors used for research, training, and radioisotope production; nuclear fuel-cycle facilities; nuclear and radioactive 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 non-power reactors, radioisotopes, and cybersecurity. The U.S. Department of Homeland Security National Protection and Programs Directorate's 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

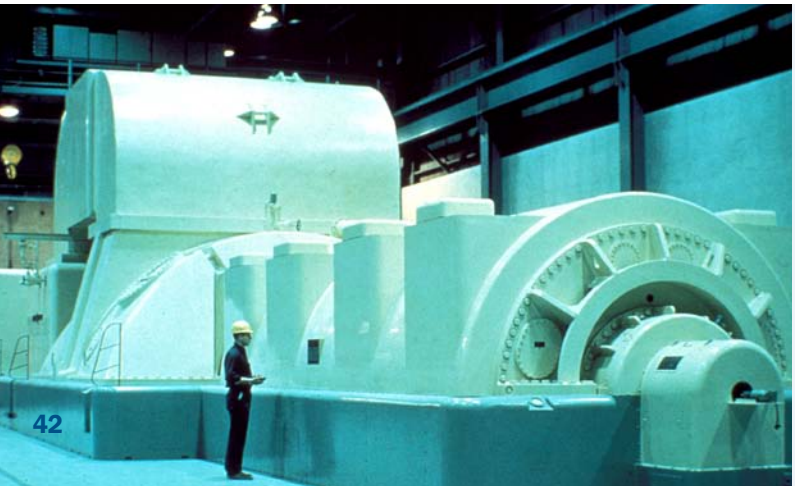
To ensure the safety, protection, and resilience of the Nuclear Sector, partners work together to achieve the following goals:

- 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 this information 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 to, 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 planning for additional Integrated Comprehensive Exercises following the 2010-2011 Integrated Pilot Comprehensive Exercises at Donald C. Cook Nuclear Power Plant and Indian Point Energy Center.
- Installed voluntary security enhancements by the National Nuclear Security Administration (NNSA) at seven non-power reactors in Fiscal Year 2010 (FY 2010).
- Completed the objectives and deliverables under the Nuclear Government and Sector Coordinating Councils–Joint Radioisotopes Subcouncil Focus Groups on the transportation of radioactive material, tracking of sealed sources, and removal and disposition of disused sources.
- Developed and submitted to Congress the *2010 Radiation Source Protection and Security Task Force Report* on the security of radioactive sealed sources.
- Recovered more than 27,800 disused radioactive sources (more than 800,000 curie) since 1997, including 3,158 sources in FY 2010.
- Implemented security enhancements at 256 U.S. buildings with high-priority radiological materials through the NNSA as of April 25, 2011.
- Installed in-device delay kits to impede the unauthorized removal of high-risk, cesium-chloride radioactive sealed sources from medical and industrial irradiators—to date, a total of 245 irradiators have received a retrofit kit; NNSA has been working with 60–80 volunteers per calendar year to implement the enhancements; and the three largest irradiator manufacturers have agreed to include the delay kits on newly produced units.
- Implemented the National Source Tracking System, which provides administrative accountability for more than 75,000 high-risk radioactive sources.



"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."

Source: 2011 Nuclear Sector Annual Report

Key Initiatives

The Nuclear Sector partners are implementing numerous protective programs and initiatives to help sustain the robust security posture of sector assets while addressing emerging risks. Key initiatives within the sector include:

- 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 and biennial emergency preparedness exercises.
- Enhancing the knowledge of first responders at facilities with nuclear or radioactive materials through the Alarm Responder Training Program and tabletop exercises.
- Conducting baseline and force-on-force security inspections to assess nuclear plants' ability to defend against the Nuclear Regulatory Commission's Design Basis Threat.
- Assessing the adequacy of State, local, and tribal government emergency plans through the Federal Emergency Management Agency's Radiological Emergency Preparedness Program.
- Conducting Federal Bureau of Investigation outreach visits to select facilities housing risk-significant radioactive materials and special nuclear material.
- Recovering; exchanging; recycling; and disposing of 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 work collaboratively with sector stakeholders to identify, prioritize, and pursue mission-essential research and development needs.
- Continue to coordinate with State and local authorities as well as 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 Cyber Systems Security in the Nuclear Sector*, modeling roadmaps created for the Chemical, Energy, and Water Sectors.
- Remain cognizant of efforts taken pursuant to recommendations of the Removal and Disposition of the Disused Sources Focus Group relating to 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 enhance supplies of key radioisotopes, such as Molybdenum-99.
- Recover; exchange; recycle; and dispose of excess, unwanted, abandoned, or orphaned radioactive sealed sources.

"All 65 of the Nation's commercial nuclear power plants submitted their cybersecurity plans, including a proposed implementation schedule by the November 23, 2009 deadline. During 2010, [the Nuclear Regulatory Commission] worked with these licensees, as well as [the Nuclear Energy Institute], to address more than 70 requests for additional information in the process of approving the plans and schedules."

Source: 2011 Nuclear Sector Annual Report

GCC MEMBERS

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

SCC MEMBERS

- American Association of Physicists in Medicine
- Arizona Public Service
- Constellation Energy
- Covidien
- Dominion
- Edison Electric Institute
- Edlow Intl.
- Entergy
- Exelon
- General Electric Hitachi
- Michigan State University
- Nuclear Energy Institute
- Oregon State University
- Purdue University
- QSA-Global
- Rutgers University
- Security Engineering Associates
- Southern Nuclear Company
- Tennessee Valley Authority
- University of Missouri-Columbia
- University of Pennsylvania
- USEC, Inc.

POSTAL AND SHIPPING SECTOR

Partnership

The Postal and Shipping (P&S) Sector is an integral part of the Nation's economy. The United States Postal Service (USPS) estimates that the mailing and shipping industry is a $1 trillion per year business that represents 7 percent of the U.S. economy and directly employs approximately 1.8 million people as well as, indirectly, an additional 5 million workers who develop; design; and produce advertising, catalogs, and letters. As the Sector-Specific Agency, the Transportation Security Administration (TSA) collaborates with the members of the P&S Sector Coordinating Council (SCC) and P&S Sector Government Coordinating Council (GCC) to improve overall sector security. The P&S Sector SCC is currently composed of USPS, FedEx Corporation, United Parcel Services of America, Inc., and DHL International. The P&S Sector GCC is composed of the U.S. Department of Homeland Security (including TSA, Office of Infrastructure Protection, Science and Technology Directorate, Management Directorate, Office of Intergovernmental Affairs, and U.S. Customs and Border Protection); U.S. Department of Health and Human Services; U.S. Department of Commerce; Federal Bureau of Investigation; U.S. Department of the Interior; U.S. Department of Defense; U.S. Department of Transportation; and a representative of the State, Local, Tribal, and Territorial GCC.

Vision

Ensure continuity of operations, ease of use, and public confidence in the P&S Sector by creating a multilayered 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 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 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 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 the implementing organization 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 and develop continuity of operations plans to ensure that the sector can continue to move parcels and letters to intended recipients.
- Identify critical commodities that must be delivered to enable an effective response to a 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:

- Responded to the threat from packages originating in Yemen with Security Directives and Emergency Amendments to ensure the safety of aircraft, personnel, and the public.

"The P&S Sector represents 7 percent of the U.S. economy and directly employs approximately 1.8 million people and an additional 5 million in support roles in developing, designing, and producing advertising, catalogs, and letters."

Source: 2011 Postal and Shipping Sector Annual Report

"Clustered-Computing Analysis Platform is a state-of-the-art forensics analysis platform for examining and analyzing digital evidence. Postal Inspectors are using this tool to shorten the time needed to conduct large-scale cyber investigations."

Source: 2011 Postal and Shipping Sector Annual Report

- Established working groups composed of domestic and international agencies and industry partners to focus on refining procedures and implementing technology to reduce the risk of terrorism and increase system resilience.
- Initiated a study to evaluate the security of U.S. mail transported on domestic passenger aircraft.
- Conducted security assessment reviews at hundreds of sector facilities nationwide.
- Participated in tabletop exercises and full-scale exercises at postal facilities nationwide, including the National Level Exercise 2011 and Cyber Storm III.
- Prepared the 2010 Postal and Shipping Sector Annual Report.
- Participated in two Critical Infrastructure Partnership Advisory Committee meetings.
- Reviewed the status of sector programs and GCC structure and membership to make recommendations for strengthening its charter.
- Conducted outreach to sector components not represented on the SCC.
- Responded to dozens of emergencies in Fiscal Year 2010 related to hurricanes, floods, fires, and other incidents.
- Established communications, a secure temporary delivery system, and continued relief efforts, ensuring proper standards for delivering and deploying equipment donations in Haiti following the major earthquake in 2010.

Key Initiatives

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

- 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's Cities Readiness Initiative.
- Improving sector resilience.
- Enhancing emergency preparedness.
- Facilitating the sharing of security information.

Path Forward

The P&S Sector faces international and domestic threats that involve using the sector's open access to reach targets. The sector faces challenges in securing numerous and easily accessible assets, large and diverse information systems, and a wide array of transportation systems. It is also challenged by a changing market that affects its economic viability.

To move forward in securing its resources, the sector will:

- Revisit sector goals for applicability under current threats.
- Review the Risk Mitigation Activities to align them with the goals and plans for moving forward and the ability to accurately measure progress.
- Engage the analytical community to provide regular threat analyses.
- Engage sector partners to assess threats, vulnerabilities, and consequences.
- Identify a methodology for developing assessments of dependencies and interdependencies.
- Engage the sector in assessing sector dependencies and interdependencies.
- Continue to engage partners in the international community in strengthening the supply chain that carries inbound and outbound international mail.
- Develop and refine changes in technology, processes, and policies to improve the resilience of the sector and the mitigation of threats.
- Foster communication channels supporting the resultant changes, as well as alerts and responses.
- Complete a study assessing the risks of mail transported on domestic passenger aircraft and implement next steps that emerge from the study.
- Complete a market survey of the mail couriers industry.
- Initiate a market study of mailrooms to understand the stakeholders and their characteristics and develop a plan to engage the industry within the National Infrastructure Protection Plan framework, identifying where security and resilience can be improved.
- Interact with other segments of the sector (e.g., couriers, mailrooms) to assess their needs regarding risk mitigation and the best means to engage them.
- Identify and define sector training and communications requirements that will allow sector components (e.g., integrated service providers, mailers, couriers, package handlers, mailroom operators, and government mailing operations) to improve the preparedness, resilience, and security of their operations.
- Ensure that timely threat information is effectively disseminated and shared.
- 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 effective.
- Understand the full scope of cybersecurity issues and vulnerabilities, develop mitigation strategies, and communicate cybersecurity improvement programs to the sector.

"In Fiscal Year 2010, the Postal Inspection Service conducted 24 Tabletop Exercises at postal facilities nationwide to evaluate response capabilities resulting from a Biohazard Detection Systems Response, Pandemic Influenza, and Bomb Threat scenarios. The Tabletop Exercises were augmented by 36 full-scale exercises and drills that ensure the Postal Inspection Service can quickly respond to the needs of the Postal Service in any emergency."

Source: 2011 Postal and Shipping Sector Annual Report

GCC MEMBERS

- 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

SCC MEMBERS

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

TRANSPORTATION SYSTEMS SECTOR

Partnership

The Transportation Systems Sector is a vast, open network of interdependent systems that 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 five transportation modes: aviation, mass transit and passenger rail, highway and motor carrier, freight rail, and pipeline. The GCC consists of members from key Federal, State, and local agencies. The sector-level representation during the prior year has been managed at the modal level, where the subsector SCCs are the primary coordination venue for the private sector under the Critical Infrastructure Partnership Advisory Council; other private sector outreach mechanisms—such as national advisory councils or committees—may also be used for collaboration, cooperation, and communication, when appropriate. The Transportation Security Administration (TSA) 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 U.S. Department of Transportation provides Federal leadership on the sector's preparedness for natural disasters and in emergency response and recovery support functions.

In 2010, the Transportation Systems Sector-Specific Plan (TS SSP) was updated, encouraging wider participation in risk reduction decisionmaking activities and building upon programs and initiatives that reduce the sector's most significant risks in an efficient, practical, and cost-effective manner. Notably, the TS SSP consists of a base plan and six modal annexes that consolidate strategic planning and infrastructure protection requirements.

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 its security posture. These improvements include the following:

- Expanded infrastructure security coverage through thousands of Visible Intermodal Prevention and Response team deployments.
- Expanded the "If You See Something, Say Something" campaign to public transportation venues.
- Achieved significant progress in implementing additional screening measures and new procedures that met the Implementing Recommendations of the 9/11 Commission Act of 2007 to include the Secure Flight watch list matching program, Certified Cargo Screening Program, and Next Generation Air Transportation System.
- Completed 26 assessments of critical bridges to facilitate risk reduction programming decisions through the partnership of bridge owners and operators and TSA.
- Reduced Toxic Inhalation Hazard (TIH) cargo risks by 93 percent for high-threat urban areas since the 2006 baseline was released.
- Established a Joint SCC and GCC Information Sharing Working Group that developed the Transit and Rail Intelligence Awareness Daily report produced by the Public Transportation (PT) and Surface Transportation Information Sharing and Analysis Centers (ISAC).
- Provided financial support for PT-ISAC initiatives through TSA.

"On October 27, 2010, in Sana'a, Yemen, an unidentified woman dropped off two packages—one at a FedEx office and one at a [United Parcel Service] office. Both firms used a combination of passenger and cargo aircraft to transport the packages toward their destination—Chicago. The next day, while the packages were still en route, authorities in Dubai and Great Britain inspected the packages and discovered improvised explosive devices hidden in the toner cartridge of a laser printer. Both devices used cell phones as initiators and pentaerythritol tetranitrate as main charges. This incident highlights the enduring threat associated with both the Transportation Systems Sector as a whole and the aviation mode in particular."

Source: 2011 Transportation Systems Sector Annual Report

- Partnered with maritime authorities in 64 countries to assess compliance with international requirements and to increase the security of commerce bound for the United States through the International Port Security Program.
- Completed 12 voluntary Pipeline Corporate Security Reviews and re-inspections of 72 major pipeline systems through the collaboration of the Nation's top 100 pipeline operators and TSA.
- Conducted 96,000 Maritime Security and Response Operations activities in 2010, which included screening more than 257,000 commercial vessels and 71 million crew members and passengers for terrorist and criminal associations prior to arrival in U.S. ports.
- Utilized the Maritime Security Risk Analysis Model (MSRAM) to support decisionmaking and encourage both asset-specific protection measures and area-wide security measures and response capabilities.

Key Initiatives

The Transportation Systems Sector is undertaking a 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:

- Screening and vetting of transportation workers through the Transportation Worker Identification Credential initiative and Hazmat Threat Assessment Program.
- Securing critical physical infrastructure through the National Tunnel Security Initiative, general aviation security measurements, and Area Maritime Security Plans.
- Reducing freight rail risks using global positioning system technology on TIH cargo shipments.
- Leveraging technologies to screen travelers through Secure Flight and the deployment of checkpoint screening technology.
- 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 refining and expanding risk methodologies, such as the Bridge Criticality Tool, MSRAM, 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.
- Initiating a Cyber Defense Enhancement Initiative to identify; assess; and manage threats, vulnerabilities, and consequences to communications information and control systems within the marine transportation system and maritime critical infrastructure.
- Supporting the development of European Union and Canadian engagement on critical infrastructure protection, including supply chain security, and sharing of best practices and tools.

Path Forward

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

- Engage with sector and transportation owners and operators in strategic partnerships to develop efficient and effective security solutions.
- Enhance information sharing and collaboration among State, local, tribal, and territorial partners in order to detect or deter unknown and evolving threats from both domestic and foreign adversaries.
- Publish a Notice of Proposed Rulemaking that would require certain owners and operators engaging in surface transportation to provide security training to their security-sensitive employees.
- Continue to work with the intelligence community to efficiently incorporate reliable intelligence into daily security responsibilities.
- Conduct periodic sector-wide risk assessments, including cyber-system assessments.
- Develop sector performance outcomes and metrics.
- Collaborate with sector owners and operators to increase cybersecurity awareness and understanding and encourage the use of tools, audits, and assessments.
- Enhance international collaboration and supply chain security vis-à-vis international engagement with partners to increase knowledge and application of risk-based approaches and, in coordination with the U.S. Department of State, work to effectively integrate and align critical infrastructure objectives with overall U.S. foreign policy.

"The sector used the joint Research and Development and Cybersecurity Working Groups to provide better channels for discussion and collaboration regarding strategies, technology development and deployment, and priorities in the mentioned [risk mitigation activity] areas. The Transportation Systems Sector [Government Coordinating Council] held one meeting in 2010. The modal GCCs and [Sector Coordinating Councils] remain the primary means of collaboration with owners and operators as there is no sector-level SCC. In several modes, advisory committees registered under the Federal Advisory Committee Act to provide an alternative channel for collaboration. The sector also engaged owners and operators through ad-hoc, joint committees to deal with risk assessments of scenarios used for [Transportation Sector Security Risk Assessment]."

Source: 2011 Water Sector Annual Report

"Last year, [U.S. Customs and Border Protection (CBP)] seized a trucking shipment containing a large quantity of marijuana. Using [Automated Targeting System], CBP tracked other cargo originating from the same shipper and was able to identify a vessel containing a large quantity of cocaine."

Source: 2011 Water Sector Annual Report

TRANSPORTATION SYSTEMS SECTOR

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

AVIATION MODE SCC MEMBERS

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

HIGHWAY AND MOTOR CARRIER MODE SCC MEMBERS

- American Bus Association
- American Chemistry Council
- American Logistics Aid Network
- American Petroleum Institute
- American Trucking Associations
- The BusBank
- Con-Way, Inc.
- Detroit-Windsor Truck Ferry
- First Student, Inc.
- Institute of Makers of Explosives
- 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 Express
- SLT Express
- Taxicab, Limousine & Paratransit Association
- Tri-State Motor Transit Company

HIGHWAY AND MOTOR CARRIER MODE SCC MEMBERS CONTINUED

- Truck Rental and Leasing Association
- United Motorcoach Association

MASS TRANSIT MODE SCC MEMBERS

- American Public Transportation Association
- Berks Area Reading Transportation Authority
- Capital Metropolitan Transportation Authority
- Community Transportation Association of America
- Dallas Area Rapid Transit/Trinity Railway Express
- Hampton Roads Transit
- Rock Island County Metropolitan Mass Transit District
- Metropolitan Transportation Authority
- New Jersey Transit Authority
- San Francisco Municipal Transportation Agency
- The Port Authority Trans-Hudson Corporation
- 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 and Williams

RAILROAD MODE SCC MEMBERS

- American Short Line and Regional Railroad Association
- Amtrak
- Anacostia and Pacific Company, Inc.
- Association of American Railroads
- BNSF Railway Company
- Canadian National Railway Company
- Canadian Pacific Railway
- CSX Transportation
- Genesee & Wyoming, Inc.
- 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. Successful attacks on Water Sector assets could result in a large number of illnesses, casualties, or an interruption in 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. These entities collaborate and coordinate effectively in order to assist drinking water and wastewater utilities increase resilience and be prepared to prevent, detect, respond to, and recover from all hazards. 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. The GCC 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 for the Water Sector and works with utility owners and operators and industry representatives to ensure that Water Sector protection and resilience strategies are effective and practical for all.

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.

Goals

The following goals were developed in support of the sector's vision and help provide the basis for ongoing risk management activities:

- Sustain protection of public health and the environment.
- Recognize and reduce risks.
- 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. The sector's accomplishments over the past year include the following:

- Completed the first drinking water contamination warning system pilot in Cincinnati through EPA's Water Security Initiative—evaluation of data and publication of results from this pilot are ongoing.
- Deployed four additional drinking water contamination water system pilots—evaluation activities for these pilots are underway.
- Conducted a second full scale exercise in Federal Emergency Management Agency Regions 9 and 10, which included the participation of 25 Federal, State, local, and commercial laboratories.
- Upgraded and revised the existing three Water Sector risk assessment methodologies to ensure consistency with the 2007 Risk Analysis and Management for Critical Asset Protection Sector-Specific Guidance for Drinking Water and Wastewater Systems.
- Developed an all-hazards risk assessment Standard for Risk and Resilience Management of Water and Wastewater Systems (J100 Standard).
- Convened a Water Sector Risk Assessment Methodology/Standard Examination Workgroup to examine further necessary modifications to the Water Sector Risk Assessment Methodologies based on the J100 Standard.
- Completed development of the Water Health and Economic Analysis Tool drinking water module for hazardous gas and loss of operating assets scenarios.
- Established one new Water/Wastewater Agency Response Network (WARN) for a total of 48 WARNs.
- Supported eight WARN tabletop exercises (TTXs) as of May 2011 and is planning to support an additional eight TTXs.
- Conducted 20 Incident Command System (ICS) and National Incident Management System (NIMS) Water Sector-specific training courses on-location to train users on how principles of ICS/NIMS can be effectively used in Water Sector-specific emergency response situations.
- Sponsored a second Water Terrorism Training in Chicago—on behalf of the EPA and the Federal Bureau of Investigation—to assist in preparing law enforcement personnel for terrorism incidents which affect the Water Sector.
- Conducted 17 Site Assistance Visits and 104 Enhanced Critical Infrastructure Protection visits using the Infrastructure Survey Tool.

"Water Sector partners have developed a comprehensive all-hazards program to address risk in the sector. The program includes a suite of risk assessment tools, training, research initiatives, outreach materials, and technical and financial assistance to help drinking and wastewater utilities identify and better protect their key components."

Source: 2011 Water Sector Annual Report

"[The] Water Environment Federation, under a cooperative agreement with the Federal Emergency Management Agency, is providing a cross-sector interdependencies and emergency response training program to assist Water Sector utilities in building sustained, resilient local and regional partnerships across critical infrastructure sectors."

Source: 2011 Water Sector Annual Report

- Completed integration of the National Environmental Methods Index for Chemical, Biological, and Radiological Methods data into the Water Contaminant Information Tool in order to make all of the data available to the Water Sector in one robust tool for use during an emergency response.
- Developed an operational framework that identifies the functions and value of the Water Sector GCC and serves as a resource to communicate the GCC's purpose to new participants, reinvigorate commitment to GCC efforts, and renew focus for current and future activities.

Key Initiatives

The Water Sector continues to focus efforts on utilities that service high-population areas. Sector partners, working collaboratively, continue to strive to minimize obstacles that all utility owners and operators may face while trying to implement protective program actions. Key initiatives within the sector include:

- Conducting pilots for drinking water contamination warning systems in five major cities across the U.S.
- Conducting protection and resilience efforts including emergency planning, training, exercises, laboratories, mutual aid, vulnerability assessments, security enhancements, contaminant identification, notification, and response and recovery.
- Promoting a broad range of water security and preparedness-related efforts through journal articles, electronic newsletter announcements, conference presentations, exhibits, and Web site enhancements, as well as through the Water Information Sharing and Analysis Center.
- Developing tools and extensive training programs to help utilities enhance their emergency response preparedness and communicate with local first responders and public health providers during an incident response; 500 participants were trained in ICS and NIMS on-location during the reporting period.

"Water Sector partners are encouraging local utilities in every State to establish intrastate mutual aid and assistance agreements to enhance preparedness and improve incident response and also to provide training and exercises to help maintain the operation of the mutual aid networks. The Water Sector has sponsored regional workshops and other outreach to provide information on how to develop a Water/Wastewater Agency Response Network."

Source: 2011 Water Sector Annual Report

- Participating in Site Assistance Visits, the Buffer Zone Protection Program, and the Enhanced Critical Infrastructure Protection Program.
- Developing a laboratory network capable of providing analytical support and the capacity necessary to process an influx of samples during an emergency.
- Initiating the development of a decisionmaking framework and flowcharts for decontamination for water utilities, responders, and other decisionmakers.

Path Forward

The Water Sector is implementing various programs to enhance the protection and resilience of its assets, including the following:

- 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 Critical Infrastructure Partnership Advisory Council working groups.

GCC MEMBERS

- Association of State and Interstate Water Pollution Control Administrators
- Association of State and Territorial Health Officials
- Association of State Drinking Water Administrators
- Environmental Council of the States
- National Association of County and City Health Officials
- National Association of Regulatory Utility Commissioners
- U.S. Department of Agriculture
- U.S. Department of Defense
- U.S. Department of Health and Human Services
- U.S. Department of Homeland Security
- U.S. Department of the Interior
- U.S. Department of Justice
- U.S. Department of State
- U.S. Environmental Protection Agency

SCC MEMBERS

- American Water
- American Water Works Association
- Artesian Water Company
- Association of Metropolitan Water Agencies
- Bean Blossom-Patricksburg Water Corporation

SCC MEMBERS CONTINUED

- Boston Water and Sewer Commission
- Breezy Hill Water and Sewer Company
- California Water Service Co.
- City of Portland Bureau of Environmental Service
- Greenville Water System
- King County Department of Natural Resources and Parks
- National Association of Clean Water Agencies
- National Association of Water Companies
- National Rural Water Association
- New York City Department of Environmental Protection
- Northeast Ohio Regional Sewer District
- Onondaga County Water Authority
- Prince William County Service Authority
- Trinity River Authority of Texas
- United Water
- Water Environment Federation
- Water Environment Research Foundation
- Water Research Foundation

The National Protection and Programs Directorate's Office of Infrastructure Protection leads the national effort to mitigate terrorism risk to, strengthen the protection of, and enhance the all-hazard resilience of the Nation's critical infrastructure.

Learn more at www.dhs.gov/criticalinfrastructure.

Homeland Security