CRITICAL INFRASTRUCTURE PARTNERSHIP ADVISORY COUNCIL

ANNUAL UPDATE

2012

Homeland Security

Critical Infrastructure Partnership Advisory Council
2012 ANNUAL UPDATE

CONTENTS

CRITICAL INFRASTRUCTURE PARTNERSHIPS

INTRODUCTION

The Nation's critical infrastructure is diverse and spans multiple sectors that include agriculture, chemical facilities, communications, drinking water, electric power, and transportation systems. These sectors produce a significant portion of the gross domestic product, and protecting the attendant infrastructure is essential to the national economy. Further, since most of the Nation's critical infrastructure is privately owned and operated, public-private partnerships are necessary to protect infrastructure, prepare for and respond to events, and build resilience.

The National Infrastructure Protection Plan (NIPP) provides a unifying framework for these partnerships that integrates a range of efforts designed to enhance the safety of critical infrastructure. The figure below illustrates the Sector Partnership Model established by the NIPP to facilitate close cooperation and foster trusted relationships to manage risks in an inherently complex environment.

Pursuant to section 871 of the Homeland Security Act of 2002, the U.S. Department of Homeland Security (DHS) established the Critical Infrastructure Partnership Advisory Council (CIPAC) to support implementation of the NIPP and activate the Sector Partnership Model. CIPAC provides a legal framework under which private sector partners may voluntarily collaborate with Federal Government partners on critical infrastructure efforts. CIPAC activities include:

- Planning and implementing infrastructure protection and resilience programs;
- Coordinating operational activities, including incident response and recovery; and
- Assisting in the development of national infrastructure policies, plans, and programs.

This *Annual Update* describes CIPAC's function and contribution and summarizes 2012 private- and public-sector protection and resilience initiatives and accomplishments of the four cross-sector partnership councils and 18 critical infrastructure sector partnerships.

CIPAC STRUCTURE

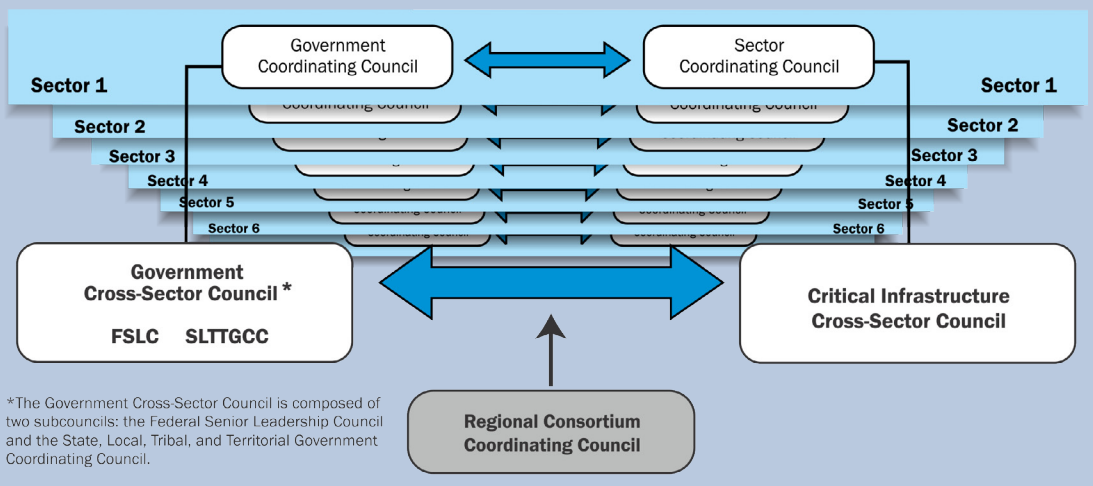
CIPAC members are organizations representing the critical infrastructure cross-sector and sector councils identified in the NIPP Sector Partnership Model.

Cross-Sector Partnerships

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 consist of the following councils:

- The ***Critical Infrastructure Cross-Sector Council*** consists of the leadership of each of the Sector Coordinating Councils (SCCs) and addresses cross-sector issues and interdependencies among the SCCs.
- The ***Government Cross-Sector Council (GCSC)*** addresses interagency, cross-sector issues, and interdependencies among the Government Coordinating Councils (GCCs), and is composed of two subcouncils: the Federal Senior Leadership Council (FSLC) and the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC).
  - The ***FSLC*** consists of senior leadership representatives from Federal agencies that are relevant to critical infrastructure protection and resilience and the Chairs/Vice-Chairs of the Sector-Specific Agencies (SSAs). SSAs work with DHS to implement the Sector Partnership Model and Risk Management Framework, develop protective programs and related requirements, and provide sector-level protection guidance.
  - The ***SLTTGCC*** consists of homeland security directors or their equivalent representatives from State, local, tribal, and territorial governments (SLTT).
- The ***Regional Consortium Coordinating Council (RCCC)*** addresses 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. The RCCC consists of regional private sector consortiums at the State or metropolitan level.

National Infrastructure Protection Plan Sector Partnership Model



*The Government Cross-Sector Council is composed of two subcouncils: the Federal Senior Leadership Council and the State, Local, Tribal, and Territorial Government Coordinating Council.

Sector Partnerships

The 18 sectors are organized as SCCs and/or GCCs, as appropriate to their sector. These sector-specific councils include representatives from the private and public sectors, respectively.

- An ***SCC*** is the principal entity for private sector owner and operator organizations or their representative trade associations to coordinate among themselves and with the government on critical infrastructure protection and resilience activities and issues within a sector.
- A ***GCC*** is the government counterpart to the SCC, which includes representatives of Federal, State, local, and tribal entities. GCCs facilitate interagency and cross-jurisdictional coordination among government critical infrastructure partners within a sector.

CIPAC FUNCTION AND CONTRIBUTION

CIPAC is both a communication forum and a legal framework by which public and private partners may have real-time, continuous communications and open dialogue. As a communication forum, CIPAC provides an opportunity for private sector partners across the sectors to meet voluntarily with key Federal Government stakeholders to share information and coordinate efforts. As a legal framework, CIPAC ensures the security and confidentiality of sensitive information and recommendations shared between the private and public sectors.

Contribution as a Communication Forum

Private sector participation in the critical infrastructure mission is essential to strategic planning and effective information sharing. The number of participants, cross-sector engagements, and products of the engagements indicate the effectiveness and utility of CIPAC as a public-private communication forum. Highlights of growth and achievements include:

- CIPAC member institutions have increased by 55 percent over the last four years, from 643 in 2009 to 997 in 2012.
- Councils and their working groups held 669 meetings in 2011, a 6 percent increase from 2010. As a further indication of CIPAC's growth, since the beginning of 2012, 607 meetings have already been conducted.
- The FSLC and the SLTTGCC held a joint meeting of the GCSC in March 2012 to discuss issues of shared interest among government partners.
- SLTTGCC leadership presented areas of common interest at a Critical Infrastructure Cross-Sector Council meeting for future action.
- The number of active users on the Critical Infrastructure Information Sharing Environment's delivery platform, the Homeland Security Information Network-Critical Sectors (HSIN-CS), increased by 9 percent in 2012.
- The number of documents available on HSIN-CS to all users increased from 16,266 in 2011 to 17,412 in 2012. Approximately nine new documents are added each day.

Overall, GCCs and SCCs operating under the CIPAC framework have made advancements in strategic planning, risk management, information sharing, training and exercises, research and development, program evaluation, and sector-specific metrics development.

Contribution as a Legal Framework

In order to protect public interests, the Federal Government established public disclosure procedures that require advisory committees to meet in open session and make associated written materials publicly available. However, in matters of infrastructure protection, these procedures can hamper effective information sharing between the Federal Government and the private sector. The CIPAC legal framework, therefore, operates under procedures designed to achieve a level of openness appropriate to support the homeland security mission while maintaining a level of confidentiality needed to share sensitive critical infrastructure information.

KEY INITIATIVES AND ACTIVITIES

The CIPAC legal framework has been leveraged by the DHS National Protection and Programs Directorate's Office of Infrastructure Protection to implement three major initiatives—Regional Initiative, Critical Infrastructure Risk Management Enhancement Initiative (CIRMEI), and Nationwide Suspicious Activity Reporting Initiative—that reflect the tailoring of Federal programs to support the evolving critical infrastructure mission.

Regional Initiative

The Regional Initiative engages regional stakeholders to improve both DHS and its partners' understanding of critical infrastructure protection and resilience activities across the country and identify opportunities for DHS to support those activities. DHS is gathering feedback from regional partners to assess which programs and tools they find most useful and will incorporate that information into its budget planning process. This will assist DHS in developing and investing in programs that help its partners more effectively manage risks to critical infrastructure. As such, the Regional Initiative is now part of the Critical Infrastructure Risk Management Enhancement Initiative.

To date, the Regional Initiative has leveraged the CIPAC framework to convene 14 Critical Infrastructure Owner and Operator Focus Groups in six Federal regions. In addition to providing valuable input to DHS, these groups provided owners and operators an opportunity to build connections with peers (including State government partners) and exchange ideas and approaches to security and business continuity. The results of these focus groups were compiled into written reports widely distributed to participants and across DHS and shared with the Assistant Secretary for Infrastructure Protection. Highlights from these reports include:

- A majority of the participants have invested in perimeter monitoring or access control technologies and use risk assessments to make the business case to company executives about investing in increased security measures.

The Regional Initiative's Critical Infrastructure Owner and Operator Focus Groups:

- *Over 300 owner and operator participants representing nearly all of the critical infrastructure sectors.*
- *The Commercial Facilities and Energy Sectors were the most-often represented.*
- *State/local observers represented homeland security, emergency management, first responders, fusion center, education, health, technology, and transit entities.*

3

- A majority of participants consider exercises and training—particularly efforts that promote employee readiness and awareness—a top security priority for their company.
- Participants stressed the importance of trusted relationships, citing working alongside and developing true partnerships with peers and security directors in their sector, State homeland security offices, emergency operations centers, fusion centers, and local law enforcement agencies.
- Protective Security Advisors, who identify, assess, and monitor risk to critical infrastructure at the regional and local levels, received universal high praise for their hard work and understanding of company operations.
- Recommendations to DHS included improving Federal-State-local government coordination, enhancing information sharing with the private sector, improving the private sector's awareness of DHS programs, and offering additional education and training tools.

The Regional Initiative also drew input from the SLTTGCC Regional Reports and Joint Critical Infrastructure Partnership (JCIP) Workshops. The SLTTGCC Regional Reports will help SLTT critical infrastructure personnel learn about and benefit from the approaches used by colleagues in different regions to advance infrastructure security and resilience. These reports summarize the region's key findings in three categories: Critical Infrastructure Program Structure, NIPP Implementation, and Leveraging of Federal Programs and Needs and Requirements. The JCIP Workshops focus on how best to integrate private sector partners into the Federal programs available to implement the NIPP.

Critical Infrastructure Risk Management Enhancement Initiative

The CIRMEI drives an enhanced process for assessing the current state of critical infrastructure protection and resilience through improved measurement, reporting, and action-oriented planning. The initiative is designed to better equip DHS and its partners to make resource allocation decisions based on actual data and results, coupled with information about risks to critical infrastructure.

Starting in late 2010, DHS worked with critical infrastructure partners to collaboratively define a common set of outcome statements to describe the desired "end state" for national critical infrastructure protection and resilience. Through CIPAC, the partnership continues this collaborative effort to increase the value of annual reporting and performance measurement, and enhance the effectiveness of the critical infrastructure community's collective risk management efforts. Critical infrastructure partners have contributed to the three core elements of the CIRMEI, as follows:

- The **National Risk Profile** provides an annual outlook on the risk landscape facing the national critical infrastructure community. The analysis contained in the National Risk Profile is meant to help government and private sector decisionmakers understand the critical infrastructure risk landscape and the risks to be managed. Over the past year, DHS worked with critical infrastructure partners in the public and private sectors to develop the *National Risk Estimate for Insider Threats*.
- The **Critical Infrastructure Protection and Resilience National Annual Report (NAR)** measures and reports on the progress of critical infrastructure protection and resilience efforts across the Sector Partnership Model through a set of outcome statements and associated metrics. DHS is currently working with representatives of the SSAs to develop metrics for the outcome statements developed through the CIPAC framework in 2011. The 2012 NAR will report on progress made against the actions identified in the Critical Infrastructure Risk Management Plan.
- The **Critical Infrastructure Risk Management Plan** establishes actions and milestones for DHS, the SSAs, and SLTT partners that address the most significant opportunities to improve critical infrastructure protection and resilience, as reported in the NAR. Over the past year, DHS held facilitated working sessions with all 18 SSAs and the Executive Committee of the SLTTGCC to discuss sector and SLTT activities that align with the improvement opportunities derived from the NAR.

Nationwide Suspicious Activity Reporting Initiative

The Nationwide Suspicious Activity Reporting Initiative provides tools for stakeholders to share suspicious activity reports (SARs) with the National Infrastructure Coordinating Center (NICC). This approach leverages the capabilities of the Critical Infrastructure Information Sharing Environment, operated by DHS, to increase cross-sector visibility of potential threats that may pertain to sector stakeholders. Over the past year, advancements have been made in engaging additional sectors to report suspicious activity and enhancing the tool by which critical infrastructure partners can submit these reports to the Federal Government.

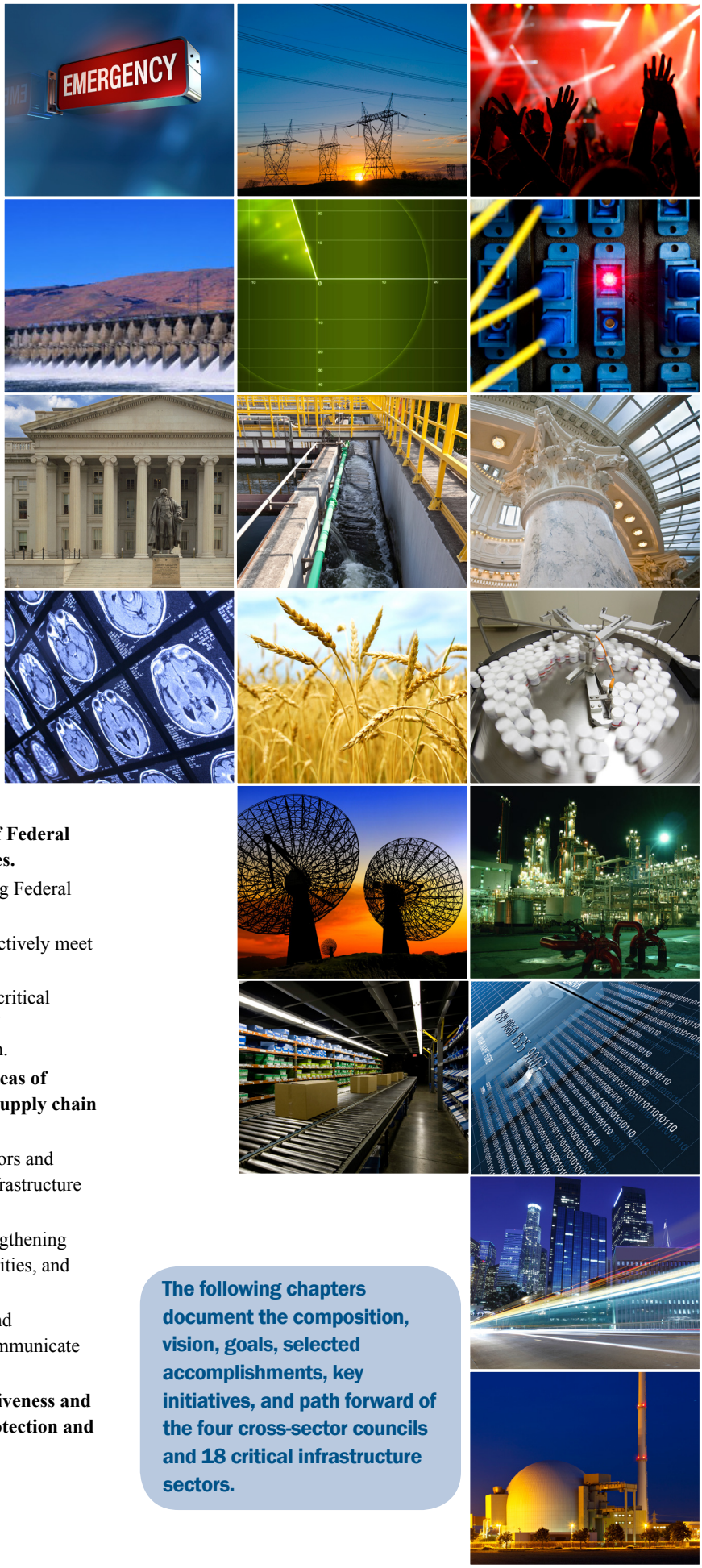
Since 2011, the CIPAC framework has facilitated information sharing with owners and operators and disseminated sector-specific tools for reporting suspicious activity. Over the past year, the Transportation Systems (Highway Motor Carrier Mode), Commercial Facilities, Chemical, and Dams Sectors were provided the capability to submit reports of suspicious activity through the SAR for Critical Infrastructure Tool (SAR Tool), which is located on HSIN-CS.

Enhancements to the SAR Tool include automating the process for transmitting SARs to facilitate receipt by the NICC and integrating the notification of suspicious activities with other Federal agencies for proper coordination. The notification integration was a result of the Chemical Sector utilizing the SAR Tool and requesting that facilities that are subject to the Chemical Facilities Anti-Terrorism Standards be identified when reporting a suspicious activity. A new version of the SAR Tool was rolled out in June 2012 and will provide additional SAR submission capabilities. As the implementation of the SAR Tool progresses, DHS will continue to engage private sector owners and operators to further improve the tool's capabilities.

2013 PRIORITIES

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 2013:

- **Maintain and promote a collaborative environment for sector partners to improve risk management and information-sharing activities.**
  - Pursue a partnership-oriented approach to refine, develop, and implement strategies and program implementation plans vital to the protection and resilience of the sectors.
  - Increase participation from partners at all levels of government and the private sector to expand information sharing.
  - Leverage existing channels of communication and build additional channels through State and local partnerships with infrastructure owners and operators.
  - Expand participation in critical infrastructure information-sharing processes and improve information-sharing effectiveness and efficiency through the development of standardizing requirements linked to specific missions.
  - Work collaboratively with sector stakeholders to identify, prioritize, and pursue mission-essential research and development needs.
- **Expand stakeholder knowledge and understanding of Federal critical infrastructure resources, tools, and capabilities.**
  - Provide guidance to SLTT governments on leveraging Federal grant programs and related resources.
  - Work with DHS to ensure that tools and training effectively meet the risk-informed needs of the partners.
  - Disseminate products and training developed by the critical infrastructure partnership to an increasing number of infrastructure owners and operators across the Nation.
- **Focus sector initiatives and investments on specific areas of concern and attention, including interdependencies, supply chain security, and cybersecurity.**
  - Improve awareness of interdependencies among sectors and agencies to help identify and address cross-sector infrastructure protection gaps.
  - Engage the critical infrastructure community in strengthening supply chain security by assessing threats, vulnerabilities, and consequences.
  - Improve the understanding of cybersecurity issues and vulnerabilities, develop mitigation strategies, and communicate cybersecurity improvement programs to the sectors.
- **Expand the use of metrics to measure program effectiveness and encourage progress toward critical infrastructure protection and resilience goals.**



The following chapters document the composition, vision, goals, selected accomplishments, key initiatives, and path forward of the four cross-sector councils and 18 critical infrastructure sectors.

CRITICAL INFRASTRUCTURE CROSS-SECTOR COUNCIL

PARTNERSHIP

The Critical Infrastructure 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 consists 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 implementation of the National Infrastructure Protection Plan (NIPP) and development of 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 protection, preparedness, and resilience of critical infrastructure assets, functions, and sectors.

GOALS

The Council pursues several key goals to increase collaboration among SCCs and the government:

- ***Partnership Leadership***: Provide proactive guidance to leverage the NIPP Sector Partnership Model to facilitate private cross-sector collaboration with the government.
- ***Cross-Sector Leadership***: Provide guidance to identify cross-sector and interdependency risks and recommend approaches to assess and manage those risks.
- ***National, Regional, State, and Local Coordination***: Foster collaboration between critical infrastructure sectors and with all levels of government to improve the security, preparedness, and resilience of the Nation's critical infrastructure. This includes coordination with the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC); the Regional Consortium Coordinating Council (RCCC); and the National Council of Information and Analysis Centers (NCI).
- ***Risk Management***: Address physical, cyber, and human cross-sector critical infrastructure protection and interdependency issues of concern to sector owners and operators.
- ***Sector Assistance***: Provide guidance to strengthen SCCs and enhance the role of the partnership framework as well as 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 the following:

- Coordinated efforts with government partners through the Cross-Sector Cybersecurity Working Group to improve and enhance the U.S. national cybersecurity profile.
- Examined cybersecurity risk management while raising awareness of cyber issues and their cross-sector impacts and interdependencies.
- Participated in joint meetings with the FSLC.
- Continued to collaborate with the White House National Security Staff during the update and revision to 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 (FEMA), 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), including the development of frameworks for prevention, protection, mitigation, response, and recovery.
- Participated actively in the design, planning, and execution of the various phases of National Level Exercise (NLE) 2012, including active engagement in the development of the exercise scenario.
- Advanced the goals and objectives of the Joint Threat Intelligence Engagement Working Group to develop procedures and protocols to improve the process and fidelity of threat intelligence information sharing and situational awareness.
- Enhanced collaboration between PCIS, the SLTTGCC, the RCCC, the NCI, and other stakeholders.
- Participated in five Joint Critical Infrastructure Partnership Workshops, sponsored by the DHS National Protection and Programs Directorate's Office of Infrastructure Protection, as a steering committee member and provided an update about the Council's mission and key initiatives at each symposium as part of the Regional Initiative.

KEY INITIATIVES

The Council organizes its efforts through several cross-sector council working groups as council member representatives on other committees to include the following:

- ***Cross-Sector Cybersecurity 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 education, awareness, and outreach efforts regarding the protection, preparedness, and resilience of critical infrastructure; coordinates an 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, sector 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.
- ***Joint Threat Intelligence Engagement Working Group***: Works with DHS to examine processes and protocols for the sharing of timely, reliable, and actionable 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 (including FEMA) and the White House National Security Staff to develop and implement the requirements identified in PPD-8.

CRITICAL INFRASTRUCTURE 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

PATH FORWARD

Important upcoming activities for the Council include the following:

- 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, including the five frameworks 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 upcoming NLEs to test the Nation's preparedness and resilience.
- Facilitate efforts to enhance collaboration between the private sector, critical infrastructure community, and the Federal Government.
- Address important issues such as access and credentialing challenges regarding incident response and consequence management, and the coordination of communication and efforts related to pending or potential threats and risks to the Nation's critical infrastructure.
- Enhance and expand efforts with other stakeholders, including the SLTTGCC, the RCCC, the NCI, and others, to improve the protection, preparedness, and resilience of the Nation's critical infrastructure.
- Expand communications and outreach activities for internal and external partners and stakeholders.
- Work with government partners to execute the partnership framework to meet the goals and objectives of the NIPP.

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 Agency (SSA) for each critical infrastructure sector as well as several additional agencies with responsibilities in critical infrastructure protection. 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 primary activities of the FSLC 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.
- Evaluating and reporting on the progress of Federal critical infrastructure protection and resilience activities in the *Sector Annual Reports* and the *Critical Infrastructure Protection and Resilience National Annual Report*.
- Meeting on a quarterly basis (or as needed to address emerging issues) and participating in annual meetings of the Government Cross-Sector Council with the SLTTGCC.

SELECTED ACCOMPLISHMENTS

Recent accomplishments of FSLC agencies include the following:

- Continued to collaborate with State, local, tribal, and territorial (SLTT) partners and critical infrastructure owners and operators to implement the Critical Infrastructure Risk Management Enhancement Initiative, which supports risk-informed decision making and measures progress against a common set of desired protection and resilience outcomes.
- Participated in the first formal meeting of the Government Cross-Sector Council, with members of the SLTTGCC Executive Committee, to discuss critical infrastructure initiatives and issues of common interest among government partners.
- Participated throughout the year in cross-sector teleconferences and Webinars with the 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 the review and revision of HSPD-7 through a subgroup of the Critical Infrastructure Protection and Resilience Interagency Policy Committee.
- Participated in interagency working groups to develop the national planning frameworks and interagency operational plans required to implement the National Preparedness System described in 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 U.S. Department of Agriculture is responsible for agriculture and food (meat, poultry, and egg products).

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

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

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

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

f. The U.S. 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 U.S. Department of Transportation and the U.S. Department of Homeland Security will collaborate on all matters relating to transportation security and transportation infrastructure protection.

OTHER FEDERAL SENIOR LEADERSHIP COUNCIL MEMBERS

- 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
- White House National Security Staff

9

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 protection and resilience planning process. SLTTGCC members seek to integrate the diverse perspectives, priorities, and needs of the SLTT community into a unified critical infrastructure protection and resilience mission.

The SLTTGCC currently has 39 members, as well as subject matter experts and the Critical Infrastructure Protection Coordinator Alliance Network, who possess institutional knowledge on a wide range of professional disciplines related to critical infrastructure protection and resilience. 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 Sector 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 water officials. The SLTTGCC 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 Government Coordinating Councils (GCCs), representing SLTT perspectives at GCC and joint GCC-Sector Coordinating Council meetings.

VISION

Foster dialogue between all levels of government to fulfill the critical infrastructure protection and resilience mission.

GOALS

The following protection and resilience goals support the overall SLTTGCC 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 the U.S. Department of Homeland Security (DHS) and other Sector-Specific Agencies (SSAs).
- 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 SLTTGCC's recent accomplishments include the following:

- Held two successful plenary sessions in September 2011 and April 2012. The former included for the first time State and local critical infrastructure protection staff, while the latter focused on strengthening the SLTTGCC's partnership with the SSAs.
- Produced four reports examining State and local critical infrastructure protection programs in three different regions of the country. The reports identify best practices and innovative approaches that other SLTT jurisdictions can draw from to bolster their own critical infrastructure protection efforts.
- Authored *Landscape Report: State Entities Participating in a Public-Private Partnership Environment*, which describes State open records and open meetings laws, or "sunshine laws," and how they affect information sharing with critical infrastructure owners and operators.
- Drafted *White Paper—Credentialing: Issues, Initiatives, and Options*, which provides the current landscape of national and SLTT credentialing initiatives and discusses options and best practices available for the enhancement of SLTT credentialing across the Nation.
- Initiated a new study to examine the level of tribal engagement in the critical infrastructure protection and resilience mission.
- Participated in the initial meeting of the Government Cross-Sector Council.
- Established a temporary working group to provide feedback to the DHS Office of Health Affairs regarding the prioritization of Anthrax Vaccine Absorbed dosing to the critical infrastructure sectors.
- Placed an SLTTGCC member on the DHS Unified Cyber Group to incorporate public sector officials operationally involved with cyber incident response.
- Provided the Federal Emergency Management Agency (FEMA) with regular feedback on the implementation of Presidential Policy Directive 8: National Preparedness (PPD-8).

KEY INITIATIVES

Between its in-person biannual plenary sessions, the SLTTGCC conducts most of its activities through nine working groups:

- Access Credentialing Working Group.
- State Asset Criteria Working Group (new in 2012).
- Cybersecurity Working Group (new in 2012).
- 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 has supported two significant initiatives designed to extend the value of its activities to SLTT critical infrastructure protection programs across the Nation: the National Protection and Programs Directorate's Office of Infrastructure Protection's Regional Initiative and the establishment of a State and local Critical Infrastructure Protection Coordinator Alliance Network.

Regional Initiative

The SLTTGCC began a two-year effort in the spring of 2011 to study the SLTT critical infrastructure protection programs in each of the 10 Federal regions. The resulting series of reports will help critical infrastructure protection staff learn about, and benefit from, the approaches that their colleagues in different regions have taken to advance infrastructure security and resilience. The results from the SLTTGCC's regional reports are the primary government input to the Regional Initiative. To date, the SLTTGCC has produced four reports through this initiative:

- Final Report: Northeast CIP Programs (March 2011)
- Final Report: Southeast CIP Programs (February 2012)
- Final Report: Region IX CIP Programs (June 2012)
- Final Report: Region VI CIP Programs (September 2012)

The SLTTGCC will complete similar reports on the State and local critical infrastructure protection programs in Federal Region VIII in calendar year 2012. Reports on the remaining regions will be completed in 2013.

In addition to its regional reports, the SLTTGCC has cosponsored with DHS two additional elements of the Regional Initiative: the Critical Infrastructure Owner/Operator Focus Groups and the Joint Critical Infrastructure Partnership (JCIP) Workshops. The SLTTGCC supported 12 focus groups and one JCIP in the CIPAC Annual 2012 reporting period.

Critical Infrastructure Protection Coordinator Alliance Network

The SLTTGCC's 2011 Fall Plenary Session revealed the need for a forum through which State and local personnel working on critical infrastructure protection issues could regularly dialogue with each other and the Federal Government. To meet this need, the SLTTGCC—with support from DHS—institutionalized the Critical Infrastructure Protection Coordinator Alliance Network. This Alliance Network, which currently includes 141 individuals from across the country, enables SLTT mission partners to network, share best practices, and provide DHS and the SSAs with regular feedback on requirements and programs. The SLTTGCC has provided members of the Alliance Network with access to its Homeland Security Information Network-Critical Sectors (HSIN-CS) page and materials, and it also sponsors a monthly Real-Time Forum (via Webinar) for the group on topics of interest to the SLTT community.

PATH FORWARD

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

- Complete its study of State and local critical infrastructure protection programs in each Federal region.
- Continue to grow the Critical Infrastructure Protection Coordinator Alliance Network and sustain the monthly Real-Time Forum series.
- Revise its May 2011 *Resilience White Paper* to reflect stakeholder input, including feedback from the SSAs and the private sector.
- Provide DHS regular feedback on its programs and tools, including recommendations associated with DHS's transition to a single assessment methodology.
- Strengthen its Sector Liaison program to ensure effective SLTT representation on the GCCs.
- Continue to evaluate HSIN-CS as a communication vehicle and recommend improvements.
- Contribute to the implementation of PPD-8.
- Broaden and diversify its pool of members and subject matter experts.

SLTTGCC MEMBERS

- Alaska Division of Homeland Security and Emergency Management
- Arizona Department of Homeland Security
- Bloomington, Minnesota Fire Department
- California Emergency Management Agency
- Charlotte, North Carolina Fire Department
- City of Seattle
- City of Tulsa
- Clark County, Nevada Office of Emergency Management and Homeland Security
- Colorado State Police, Office of Preparedness and Security
- Columbiana County, Ohio Health District
- Commonwealth of Virginia Office of Governor Robert F. McDonnell
- Delaware Department of Safety and Homeland Security
- Florida Department of Law Enforcement, Florida Fusion Center
- Georgia Emergency Management Agency
- Harris County, Texas Office of Homeland Security and Emergency Management
- Hennepin County, Minnesota Department of Human Services and Public Health
- Iowa Homeland Security and Emergency Management Division
- 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
- Michigan State Police
- Mississippi Office of Homeland Security
- 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 City Department of Information Technology and Telecommunications
- New York State Division of Homeland Security
- Nueces County, Texas Office of Emergency Management
- 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 Department of Public Safety, Division of Intelligence and Counterterrorism
- Tulalip Tribal Police Services
- Utah Department of Public Safety
- Virginia Department of Health
- West Virginia National Guard Military Authority
- West Virginia Department of Homeland Security and 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. Due to the specific challenges and interdependencies facing individual regions, and the broad range of public and private sector partners, regional efforts are often complex and diverse. To better support the implementation of the National Infrastructure Protection Plan (NIPP) at the regional level, the 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 include enhancing the physical security, cybersecurity, and personnel security of infrastructure; emergency preparedness; and overall industrial and governmental continuity and resilience of one or more States, urban areas, or municipalities. Currently, the RCCC has 23 members that represent various States and metropolitan areas.

VISION

To understand, connect, enable, and build partnerships for the protection of the critical infrastructure of the United States and the resilience of our communities.

GOALS

The RCCC identified the following 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 the cross-sector councils.
- Support DHS and critical infrastructure sector partnership communication and sharing of homeland security risk mitigation and vulnerability assessment initiatives involving members of regional consortium entities that are members of 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 and 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, as well as the Critical Infrastructure Cross-Sector Council; State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC); and the critical infrastructure sectors within CIPAC to evaluate regional interdependencies between critical infrastructure sectors that specifically impact RCCC member entities.
- Assess effective security and other preparedness measures of the regional consortia and their members and incorporate these measures, as appropriate, into an RCCC inventory that is accessible and available to all RCCC members.
- Assist in promoting 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:

- Increased membership and regional representation by approving the New England–Community Incident Preparedness Alliance for RCCC membership.
- Increased awareness of the RCCC and presented on best practices for working with the private sector at the 2012 National Homeland Security Conference.
- Maintained an interactive, dynamic, and social-media-friendly Web presence on the RCCC's Web site (http://www.RC3US.org), which utilizes the Google Maps platform to display a map of the RCCC's membership partnerships. Capabilities to interface with Facebook, Twitter, and YouTube are in development.
- Hosted the 2012 annual RCCC Plenary to coincide with the CIPAC Plenary and enable members to attend both sessions.
- Participated in five Joint Critical Infrastructure Partnership Workshops as a steering committee member and panelist. The RCCC's panel presentation focused on the RCCC's mission and key initiatives.

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 Cross-Sector Council and the SLTTGCC to improve information sharing and communication throughout the NIPP Sector Partnership and identify ways in which the three councils can leverage each other's membership and knowledge.
- Hosting Webinars to enhance partners' understanding of the roles of the RCCC, Critical Infrastructure Cross-Sector Council, and the SLTTGCC in critical infrastructure protection and resilience.
- 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.

PATH FORWARD

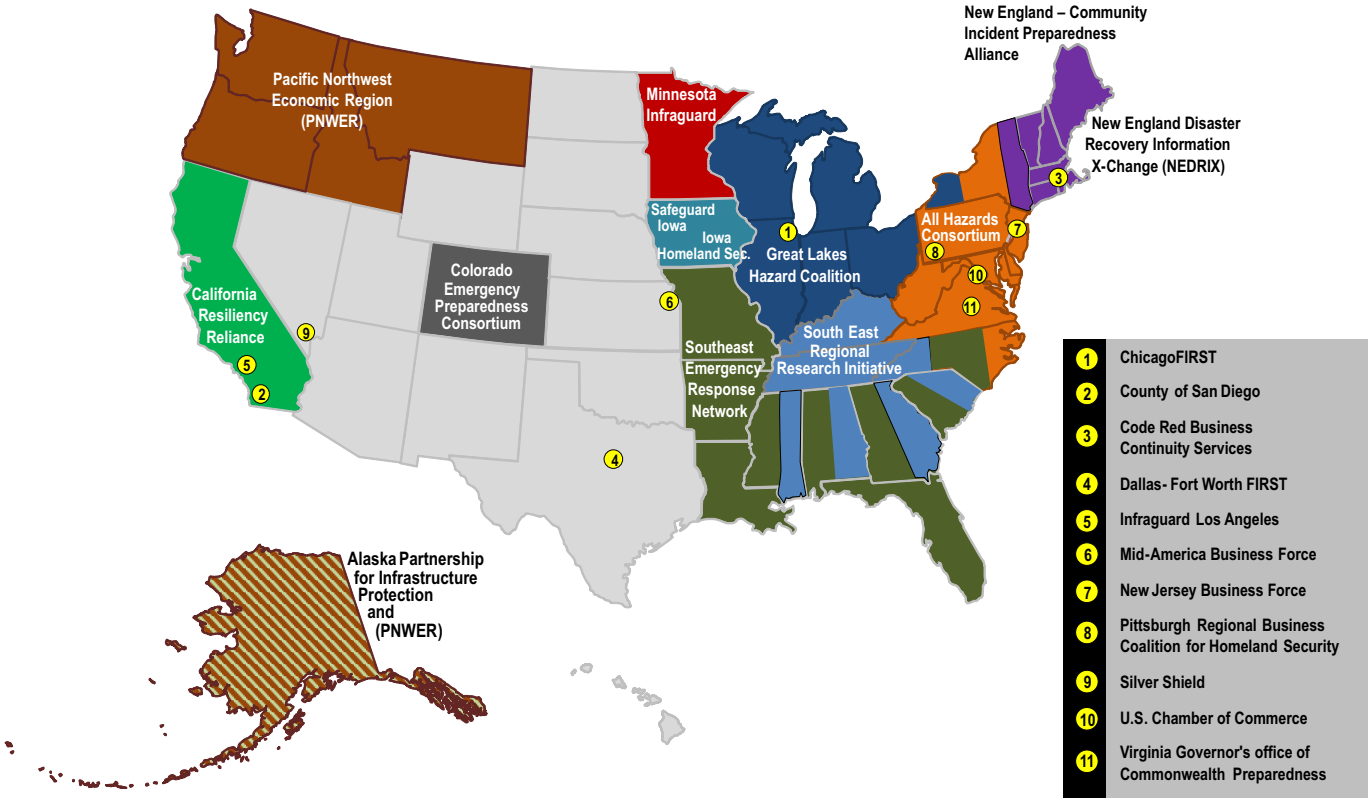
The RCCC developed an aggressive plan to accelerate its maturation throughout 2012 and beyond. Steps to move the RCCC forward in achieving its goals include the following:

- Reaching out to the critical infrastructure community as a whole to develop strong partnerships with leaders that demonstrate prolific critical infrastructure protection and resilience efforts. Examples include the Federal Emergency Management Agency Private Sector Division, the DHS National Protection and Programs Directorate's Office of Infrastructure Protection, the Federal Bureau of Investigation Public-Private Alliance Unit, the U.S. Chamber of Commerce, the American Red Cross, academic centers of excellence, and independent volunteer groups.
- Identifying additional regional partnership activities to sponsor and/or engage RCCC members and partners.
- Advancing supporting partnerships, collaborations, and tools that will provide the greatest force-multiplying effect across regional partnerships. Examples include Geospatial Information Systems and social media efforts that significantly increase situational awareness both in planning and response to events threatening the Nation's critical infrastructure.
- Continuing to build structures that will enable the RCCC to assist with national-level policy discussions that affect regional critical infrastructure entities, owners, and operators.
- Implementing a strategy for a member-hosted Webinar series to provide regional and national snapshots of specific projects around the country. The Webinars will be organized by theme, and will be concise, informative, and action-oriented. Examples of topics include the use of social media in emergency management, connecting businesses to Emergency Operations Centers, access and credentialing, and information sharing and threat analysis.

RCCC MEMBERSHIP

- Alaska Partnership for Infrastructure Protection
- All Hazards Consortium
- California Resiliency Alliance
- ChicagoFIRST
- Colorado Emergency Preparedness Consortium
- Dallas-Fort WorthFIRST
- Great Lakes Hazard Consortium
- InfraGard Los Angeles
- InfraGard Minnesota
- Mid-America Business Force
- New England Community Incident Preparedness Alliance
- New England Disaster Recovery Information X-Change
- New Jersey Business Force
- Pacific Northwest Economic Region
- Pittsburgh Regional Business Coalition for Homeland Security
- Red Business Continuity Services
- Safeguard Iowa
- San Diego County Office of Emergency Services
- Silver Shield
- Southeast Emergency Response Network
- South East Regional Research Initiative
- U.S. Chamber of Commerce
- Virginia Governor's Office of Commonwealth Preparedness

Regional Consortium Coordinating Council Map of Participants



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; Financial Services Information Sharing and Analysis Center (FS-ISAC); and 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), which serves as the sector's Government Coordinating Council. The U.S. Department of the Treasury is the Sector-Specific Agency for the Banking and Finance Sector.

VISION

To continue to improve the resilience, 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 cyber threats and 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, Energy, Information Technology, and Transportation Systems Sectors.
- Work with the law enforcement and intelligence communities, financial regulatory authorities, the private sector, and international counterparts to address current and potential threats facing financial firms.

SELECTED ACCOMPLISHMENTS

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

- Established working groups to address measures for thwarting botnets and mechanisms for ensuring high-level technical information sharing by financial institution executives as needed during major incidents.
- Reviewed potential applications for the previously developed Financial Services Threat Matrix that address impacts to market and institutional confidence, concentration, supply chain, infrastructure, geographic proximity, and technology risks.
- Enhanced cybersecurity information sharing and implemented protocols for incident response, including a major collaborative take down of cyber attackers.
- Engaged in National Level Exercise 2012, including through FS-ISAC participation.
- Participated in the 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.
- Initiated research under the previously completed memorandum of understanding on cybersecurity research developed in conjunction with the White House, U.S. Department of Homeland Security, and the National Institute of Standards and Technology 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*.

KEY INITIATIVES

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

- Identifying future operational challenges for the sector through a "long-range vision" to ensure that infrastructure owners and operators continually position themselves for a rapidly evolving threat environment.
- Utilizing a prioritized threat matrix 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 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).
- Developing a framework and methodology to identify critical financial services infrastructure by updating previous FSSCC and other sector and government work on critical infrastructure identification and risk assessments. The sector is also identifying systemically important assets, systems, and networks (including financial institutions and service providers based in the United States or abroad) that are so vital to the national economy that if they are disrupted, degraded, or destroyed, there will be severe national security or national economic impacts.

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 into 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 national cybersecurity policy issues.
- Ensure continuity of leadership and expand participation of private sector partners.
- Continue senior leadership meetings between the FSSCC and the 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 U.S. Department of the Treasury to consolidate and prioritize efforts.
- Increase committee membership and focus on the FSSCC's international functional area and related efforts across the sector.

FBIIC MEMBERS

- American Council of State Savings Supervisors
- Commodity Futures Trading Commission
- Conference of State Bank Supervisors
- Farm Credit Administration
- Federal Deposit Insurance Corporation
- Federal Housing Finance Agency
- Federal Reserve Bank of New York
- Federal Reserve Board
- National Association of Insurance Commissioners
- National Association of State Credit Union Supervisors
- National Credit Union Administration
- North American Securities Administrators Association
- Office of the Comptroller of the Currency
- Securities and Exchange Commission
- Securities Investor Protection Corporation
- U.S. Department of Homeland Security
- U.S. Department of the Treasury

FSSCC MEMBERS

- Allstate
- American Bankers Association
- American Council of Life Insurers
- American Insurance Association
- Bank Administration Institute
- Bank of America
- The Bank of New York Mellon Corporation
- Bankers & Brokers
- BATS Exchange
- ChicagoFIRST, LLC
- CITI
- The Clearing House
- The CLS Group
- CME Group

FSSCC MEMBERS CONTINUED

- Credit Union National Association
- The Depository Trust & Clearing Corporation
- DirectEdge
- Discover
- Equifax
- Federal National Mortgage Association
- Fidelity
- Financial Industry Regulatory Authority
- Financial Services Information Sharing and Analysis Center
- The Financial Services Roundtable
- Freddie Mac
- Futures Industry Association
- Goldman Sachs
- Independent Community of Bankers of America
- Intercontinental Exchange, Inc.
- International Securities Exchange
- Investment Company Institute
- JP Morgan Chase
- Managed Funds Association
- MasterCard
- Morgan Stanley
- NACHA – The Electronic Payments Association
- The NASDAQ Stock Market, Inc.
- National Armored Car Association
- National Association of Federal Credit Unions
- National Association of Insurance Commissioners
- National Association of State Credit Union Supervisors
- National Credit Union Administration
- National Futures Association
- National Stock Exchange
- Navy Federal Credit Union
- North American Securities Administration Association
- Northern Trust
- NYSE Euronext
- Omgeo, LLC
- PayPal
- Sallie Mae
- Securities Industry Financial Markets Association
- State Street Global Advisors
- Travelers
- Visa U.S.A.
- Wells Fargo

15

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. The 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. The Chemical Sector-Specific Agency (SSA), which oversees voluntary efforts under the National Infrastructure Protection Plan (NIPP), resides within the Sector Outreach and Programs Division. The SSA operates under the NIPP Sector Partnership Model, 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.

A fundamental objective of the NIPP is to protect and improve the resilience of infrastructure that has been 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, DHS continues to implement the Chemical Facility Anti-Terrorism Standards (CFATS) at sites determined to be 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 coordination between the government and the private sector 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 CFATS for the highest risk facilities in the sector (as of May 22, 2012, 3,662 facilities have been assigned a final tier and 773 are awaiting a final tier assignment).
- Coordinated the sixth annual Chemical Sector Security Summit in July 2012.
- Certified 13,912 individuals who completed the Web-based Chemical Security Awareness Training Program since its launch in July 2008.
- Adapted the Web-based Chemical Security Awareness Training Program for popular learning management systems (LMS) used by sector partners. (As of June 2012, companies reported that 16,320 trainings were completed via the LMS version.)
- Created and distributed the *Chemical Sector Industrial Control Systems Security Resource* DVD, which includes training, applicable standards, a cyber tabletop exercise, and the National Cybersecurity Division's Cybersecurity Evaluation Tool.
- Collaborated on incident management processes and information sharing during National Level Exercise 2012, an exercise in which players tested their company's cyber incident response plan and used the exercise After Action Report to inform future planning.
- Participated in a number of information-sharing initiatives, such as the National Infrastructure Advisory Council's information-sharing study and a DHS Office of Intelligence and Analysis initiative that refined the standing information needs of the sector.
- Accepted the Voluntary Chemical Assessment Tool (VCAT) as a security risk assessment tool that meets the vulnerability assessment specifications outlined in the security programs of two Chemical SCC industry associations.
- Completed the Chemical Sector Preparedness Accreditation and Certification Program (PS-Prep) Framework Guides.

KEY INITIATIVES

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

- 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 preparing best practice security information for distribution through the collaborative efforts of DHS and industry partners.
- Enhancing information sharing through the Chemical Sector Security Summit, Classified Chemical Sector Briefings, monthly suspicious activity teleconferences held jointly with the Oil and Natural Gas Subsector, the Chemical Sector Training and Resources Web site on www.dhs.gov, and the Homeland Security Information Network – Critical Sectors.
- Promoting 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.
- Improving preparedness and response capabilities by providing training opportunities through the Ammonia Safety and Training Institute and Transportation Community Awareness and Emergency Response efforts.
- Implementing the *Roadmap to Secure Control Systems in the Chemical Sector* and developing sector cyber incident management procedures.
- Developing a good practices guide with sector partners for securing chemicals in the global supply chain.

PATH FORWARD

As the Chemical Sector moves forward in protecting and enhancing the resilience of its critical infrastructure, it will take the following steps:

- 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 Sector Partnership Model to improve information sharing on chemical security legislation and harmonize security regulations across the Federal Government.
- Work to minimize the disruption to the Chemical SCC caused by the Presidential Memorandum—Lobbyists on Agency Boards and Commissions to agency heads restricting the participation of registered lobbyists in Critical Infrastructure Partnership Advisory Council meetings.
- Maximize outreach efforts to owners and operators, State chemical industry councils, and first-responder communities in order to introduce these entities and 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.

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
- The American Chemistry Council
- American Coatings Association
- American Fuel and Petrochemical Manufacturers
- BASF Corporation
- The Chlorine Institute
- Compressed Gas Association
- Council of Producers & Distributors of Agrotechnology
- CropLife America
- The Fertilizer Institute
- International Institute of Ammonia Refrigerants
- International Liquid Terminals Association
- Institute of Makers of Explosives
- National Association of Chemical Distributors
- Praxair, Inc.
- Rhodia, Inc.
- Society of Chemical Manufacturers and Affiliates

17

COMMERCIAL FACILITIES SECTOR

PARTNERSHIP

The Commercial Facilities Sector, widely diverse in both scope and function, has 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, and amusement and theme parks) that host activities which instill pride in the American way of life and develop a sense of community. Historically, emergency preparedness and 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 for 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 nonobstructive 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 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 sector 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 Risk Self-Assessment Tool (RSAT) modules specifically tailored to address risks associated with convention centers, lodging, racetracks, and theme parks and fairgrounds.
- Created *Protective Measures Guides* for the U.S. lodging industry, mountain resorts, and outdoor venues.
- Enhanced information sharing through the development of the Suspicious Activity Reporting (SAR) Tool.
- Conducted classified briefings in seven cities across the country.
- Developed the *Cybersecurity in the Retail Subsector Webinar* in collaboration with the National Cybersecurity 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.

KEY INITIATIVES

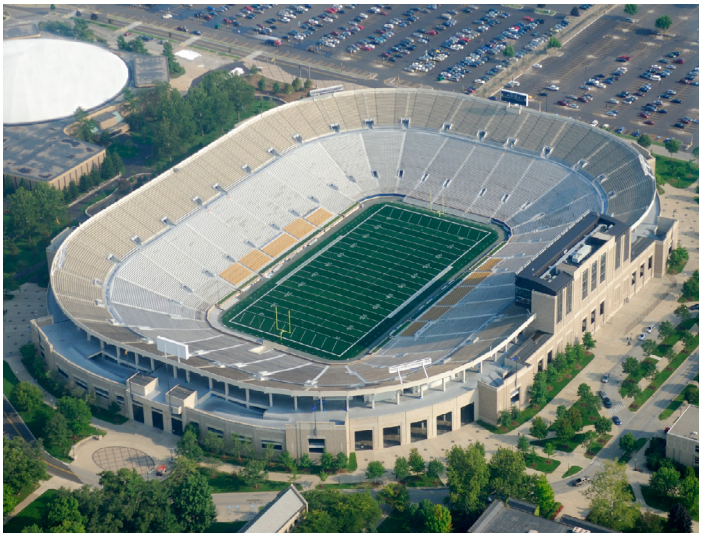
Private and public sector partners are engaging in numerous initiatives to help meet the Commercial Facilities Sector's goals. These initiatives include the following:

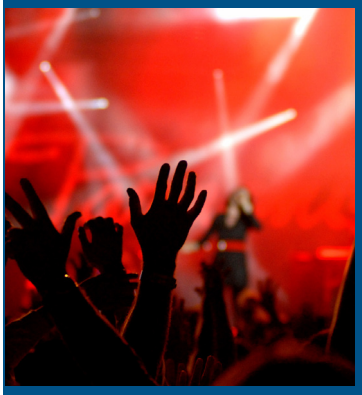
- Providing explicit risk mitigation guidance to owners and operators through DHS advisory posters, protective measures guides, *Active Shooter: What You Can Do* training materials, pandemic influenza planning documents for public assembly facilities, and the Commercial Facilities SSA outreach program.
- 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, and theme parks and fairgrounds.
- Leveraging the Commercial Facilities SAR Tool which allows commercial facility owners and operators to act as information-sharing force multipliers by providing a platform for sharing SARs with the National Infrastructure Coordinating Center.
- Sponsoring 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 initiatives such as tabletop exercises, concentrating on private sector partners that are less engaged.
- Promote the Protected Critical Infrastructure Information Program to ease the concern expressed by owners and operators 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*.





GCC MEMBERS

- Library of Congress
- 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. Secret Service
- U.S. Department of the Interior
- U.S. Department of Justice
  - Federal Bureau of Investigation
- U.S. Department of State
- U.S. Environmental Protection Agency
- U.S. Food and Drug Administration

SCC MEMBERS

- American Hotel and Lodging Association
- Beacon Capital Partners
- Building Owners and Managers Association International
- Cushman & Wakefield
- International Association of Amusement Parks & Attractions
- International Association of Fairs and Expositions
- International Association of Venue Managers
- International Council of Shopping Centers
- Major League Baseball
- Mall of America
- Marriott International
- National Association for Stock Car Auto Racing, Inc.
- National Association of Industrial and Office Properties
- National Hockey League
- National Multi Housing Council
- National Retail Federation
- NBC Universal
- Paramount Pictures
- RBC Center
- The Real Estate Roundtable
- Related Management Company
- Retail Industry Leaders Association
- Self Storage Association
- South Point Casinos
- Stadium Management Association
- Starwood Hotels & Resorts Worldwide
- Tishman Speyer Properties

COMMUNICATIONS SECTOR

PARTNERSHIP

Recent technology- and service-related innovations in the Communications Sector have enhanced national security/emergency preparedness (NS/EP) response and recovery capabilities critical to the continued operations of the Nation's mission essential functions. In addition, increasing interdependencies between the Communications and Information Technology (IT) Sectors make protecting sector assets, systems, and networks even more critical to domestic security. Communications Sector technologies include wireline, wireless, satellite, cable, and broadcasting transport networks that are part of a larger global telecommunications and IT infrastructure. These technologies and their associated infrastructure support Internet, voice, data, and other key IT and communications services. Due to the fact that the vast majority of the Nation's telecommunications infrastructure is owned and operated by the private sector, the Communications Sector has a long history of public-private partnership among its members and within the Federal Government with respect to NS/EP communications. The sector uses this partnership to foster cooperation and cultivate trusted relationships that have resulted in the successful and timely delivery of critical communications services when emergencies and disasters occur.

The National Communications System (NCS) within the U.S. Department of Homeland Security (DHS) serves as the Sector-Specific Agency (SSA) for the Communications Sector. In its role as the SSA, the NCS heads the Communications Government Coordinating Council (GCC) and is responsible for implementing the National Infrastructure Protection Plan Sector Partnership Model and Risk Management Framework, developing protective programs and related requirements, and providing sector-level critical infrastructure protection. In 2005, the communications industry formed a Sector Coordinating Council (SCC) to work with DHS; the GCC; and other Federal, State, local, tribal, and territorial entities to ensure coordination of infrastructure protection activities for the sector. SCC members represent the majority of wireline, wireless, satellite, cable, and broadcasting owners and operators, as well as major trade associations. In conjunction with GCC and SCC members, the NCS manages and participates in various communications partnerships that aim to improve all-hazards response, promote physical and cybersecurity situational awareness, and facilitate the exchange of critical information. Examples of such partnerships include the National Coordinating Center for Telecommunications and the Network Security Information Exchanges (NSIE).

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 based on its public-private partnership, the sector strives to ensure that no known physical or virtual threats pose an unmitigated 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.
- Reconstitute critical communications services rapidly in the event of disruption and mitigate cascading effects.
- Improve the sector's NS/EP posture with Federal, State, local, tribal, territorial, 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 Communications Commission's Communications Security, Reliability, and Interoperability Council.
- Conducted joint exercises and training initiatives such as Eagle Horizon, one of four major exercises conducted during National Level Exercise 2012, which tested the National Cyber Incident Response Plan.
- Updated collaborative sector documents, including the 2010 Communications Sector-Specific Plan 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, which included convening NSIE, government, and private sector representatives to focus on information sharing; issues surrounding advanced persistent threats; and best practices related to 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.
- 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 in cooperation with the Joint Telecommunications Resources Board and the Executive Office of the President.

- Led the 2012 National Sector Risk Assessment (NSRA), a joint public-private initiative that serves to improve the security and resilience of the Nation's communications systems, as well as assist decisionmakers and stakeholders in reducing risk across the Communications Sector.
- 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, local, tribal, and territorial 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 the following:

- 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, local, tribal, and territorial levels.
- Conducting joint exercises and training initiatives with government and industry partners to enhance critical infrastructure protection and response.
- Assisting international partners to further develop and improve NSIE to mitigate cyber intrusions in public telephone networks.
- Providing communications services to mitigate network congestion or disruption via priority services programs such as GETS, TSP, and WPS.
- Completing Phase I of the NSRA in summer 2012—an enhancement and update of the 2008 NSRA jointly written by government and industry partners.
- Facilitating supply chain risk management (SCRM) discussions between government and industry partners and collecting SCRM best practices through the Cross-Sector Supply Chain Working Group.

GCC MEMBERS

- Federal Communications Commission
- Federal Reserve Board
- General Services Administration
- National Association of Regulatory Utility Commissioners
- U.S. Coast Guard
- 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
- Association of Public Television Stations
- AT&T
- Century Link
- Cincinnati Bell
- Cisco Systems, Inc.
- Clearwire
- Computer Sciences Corporation
- CTIA - The Wireless Association
- Harris Corporation
- Hughes Network Systems
- Internet Security Alliance
- Intrado
- Iridium
- Juniper Networks
- Level 3 Communications
- Motorola
- National Association of Broadcasters
- National Cable & Telecommunications Association
- NeuStar
- Research in Motion
- Satellite Industry Association
- Sprint
- Telcordia
- Telecommunications Industry Association
- Telephone and Data Systems, Inc.
- Time Warner Cable
- U.S. Internet Services Provider Association
- U.S. Telecom Association
- Verizon

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 for obtaining stakeholder input for incorporation into the NSRA risk assessment updates.

21

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 a liaison from the State, Local, Tribal, and Territorial Government Coordinating Council. The U.S. Department of Homeland Security (DHS) National Protection and Programs Directorate's Office of Infrastructure Protection is the Sector-Specific Agency (SSA) for the Critical Manufacturing Sector.

VISION

The Critical Manufacturing Sector will reduce the risks through the 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 compose the critical infrastructure of the Critical Manufacturing Sector.
- Develop an up-to-date risk profile of the assets, systems, and networks within the Critical Manufacturing Sector that will enable a risk-based prioritization of protection activities.
- Develop protective programs and resilience strategies that address the risk to the Critical Manufacturing Sector without hindering its economic viability.
- Create a means of measuring the progress and effectiveness of 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.
- Continue augmentation of the Critical Manufacturing Sector's membership base to include appropriate government and private sector stakeholders and ensure all applicable information continues to be studied.

SELECTED ACCOMPLISHMENTS

Sector partners have undertaken numerous measures over the past year to increase the sector's security and resilience posture, which include:

- Created a more representative SCC by providing an outreach initiative tailored to regional small- and medium-sized manufacturers.
- Led the outreach effort to gather private sector input for the *National Strategy for Global Supply Chain Security* through the Cross-Sector Supply Chain Working Group.
- Developed tabletop exercises specifically aligned with SCC members' emergency response plans, creating opportunities for discussions among stakeholders concerning the supply chain, facility access control, and disgruntled employees.
- Completed After Action Reports following tabletop exercises that identified key areas for improvement.
- Continued two-way information sharing among SCC and GCC members through the Information Sharing Working Group, which holds monthly Webinars on key topics as identified by SCC and GCC members.
- Provided a platform for ongoing conversations regarding cybersecurity through the Cybersecurity Working Group; conversation topics have included cybersecurity resources available from the Federal Government such as the United States Computer Emergency Readiness Team, the Industrial Control Systems Cyber Emergency Response Team, the DHS National Cybersecurity Division, the DHS National Cybersecurity and Communications Integration Center, and cybersecurity exercises.
- Created a Voluntary Private Sector Preparedness Accreditation and Certification Program (PS-Prep) Working Group to review the segments of the PS-Prep Framework Guide, and provided a forum for conversations between government and the private sector, as well as between private sector entities, regarding the certification process.
- Established the Global Crisis Response Working Group at the request of the SCC to serve as a small community discussion forum in the event of an overseas crisis. This working group was inspired by the SSA's support efforts to the SCC following the Japanese earthquake and tsunami in the spring of 2011.
- Hosted the second annual Partnership Road Show, inviting SCC members to the National Capital Region to learn about available government resources for enhancing their security and resilience. Added a successful "Cyber Track" for cybersecurity professionals within the SCC.
- Created the Critical Manufacturing Cross-Border Working Group, which focuses on the northern border. Working Group members consist of SCC and GCC members, with subject matter experts participating from the Canadian government and the Canadian private sector.
- Developed the Business Continuity Planning Suite, consisting of training, automated templates, and tabletop exercises to assist businesses in maintaining operations and ensuring resilience as a result of a disruption.
- Developed the initial 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, as well as elevate awareness and understanding of threats and vulnerabilities to their assets, systems, and networks.

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 necessary information that does not unduly burden 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.
- Preparing for the 2012 Critical Manufacturing Security Conference held September 5–6, 2012.
- Collaborating, developing, and sharing appropriate threat and vulnerability information among public and private sector partners, including development of indications and warnings.
- Participating in exercises for validating communication protocols, response plans, and procedures necessary to reduce recovery time following an incident.

PATH FORWARD

To enhance the protection and resilience of its assets, the Critical Manufacturing Sector is pursuing the following activities:

- 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 the Transportation Security Administration, State homeland security advisors, State emergency managers, and others across the country to deliver the Supply Chain Security Exercise Series and SSA-sponsored programs to industry stakeholders.
- Coordinate with the Manufacturing Extension Partnership community to reach a broad network of small- to mid-sized manufacturers and offer security and resilience 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
- 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

SCC MEMBERS CONTINUED

- Delphi Corporation
- Ellanef Manufacturing
- Emerson Electric Co.
- FairChild SemiConductor
- FarSounder, Inc.
- Ford Motor Company
- General Electric Company
- General Motors
- Goodyear Tire & Rubber Company
- GrayGlass
- Hercules Heat Treating Corporation
- Intel Corporation
- ITT Corporation
- Johnson Controls, Inc.
- Kohler Company
- Lee Spring Company
- Mi-Jack Systems & Technologies, LLC
- Mini Circuits
- Navistar International Corporation
- Nichols Brothers Boat Builders
- Novelis, Inc.
- Oshkosh Corporation
- PACCAR Inc.
- 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 Corporation
- Steeler Inc.
- Summit Appliance
- TE Connectivity
- ThyssenKrupp Stainless USA, LLC
- United States Steel Corporation
- United Technologies Corporation
- Whirlpool Corporation
- Zero International

23

DAMS SECTOR

PARTNERSHIP

The Dams Sector encompasses dam projects, power plants, navigation locks, levees, mine tailings and other industrial waste impoundments, dikes, hurricane barriers, and other similar water retention and water control facilities throughout the Nation. 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 and storm surge protection, and recreation. There are more than 84,000 dams in the United States; approximately 69 percent are privately owned, and more than 85 percent are regulated by State dam safety offices. 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 Dams Sector.

The sector operates under the auspices of the Critical Infrastructure Partnership Advisory Council framework and consists of a Sector Coordinating Council (SCC) and a Government Coordinating Council (GCC). The Dams 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 in the planning, implementation, and execution of sector-wide security programs for the sector's assets. It consists of representatives from various levels of government (Federal, State, local, tribal, and territorial), including Federal owners and operators as well as State and Federal regulators of sector assets. To ensure that the Nation's community of levee owners and operators is adequately represented, the Levee Subsector Coordinating Council (LSCC) was established to represent non-Federal entities that own and operate levees and related professional organizations. In addition, the Levee Subsector Government Coordinating Council was established to serve as the government counterpart to the LSCC.

VISION

The Dams Sector will identify the measures, strategies, and policies appropriate to protect its assets from terrorist acts and enhance their capability to respond to and recover from attacks, natural disasters, or other emergencies through the development of multifaceted, multilevel, and flexible protective programs and 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 (R&D) efforts.
- Identify and address interdependencies.

SELECTED ACCOMPLISHMENTS

Sector partners have taken effective measures to maintain and enhance protection and resilience in the Dams Sector. The sector's accomplishments over the past year include the following:

- 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.
- Developed the Dams Sector Tabletop Exercise Toolbox to provide dam owners and operators with a useful exercise planning tool that maximizes the limited resources available for exercise purposes.
- Completed the San Diego Blast Damage Assessment Pilot Study in coordination with the U.S. Army Corps of Engineers and the City of San Diego.
- Completed the New Jersey Blast Damage Assessment Pilot Study in coordination with the U.S. Army Corps of Engineers and the New Jersey Department of Environmental Protection.
- Completed two comprehensive technical guidelines for consequence assessment, *Estimating Loss of Life for Dam Failure Scenarios* and *Estimating Economic Consequences for Dam Failure Scenarios*, which describe the consequence estimation approaches most commonly used in the United States and Canada.
- Conducted the fifth annual National Dam Security Forum in conjunction with the Association of State Dam Safety Officials' Dam Safety Conference held September 16 - 21, 2012, in Denver, Colorado.
- Conducted a two-day Dams Sector Research and Development Workshop where 77 representatives from the private sector; academia; national laboratories; and Federal, State, and local governments discussed current sector-wide R&D capability gaps.
- Conducted the Dams Sector Information Sharing Drill, with 123 public and private dam owners and more than 50 Federal, State, and local government representatives participating to evaluate the effectiveness of current information-sharing mechanisms across the Dams Sector.
- Continued to actively recruit members for the Homeland Security Information Network-Critical Sectors (HSIN–CS) Dams Portal, with 570 users as of June 2012.
- Continued to successfully implement Web-based Independent Study (IS) training courses, with 1,782 course completions as of June 2012: "IS- 870 Dams Sector Crisis Management" (1069 completions), "IS-871 Dams Sector Security Awareness" (373 completions), and "IS-872 Dams Sector Protective Measures" (340 completions).
- Submitted 88 suspicious activity reports (SARs) in 2011 and 11 SARs between January 1, 2012 and May 31, 2012 using the Dams Sector SAR Tool available via the HSIN–CS Dams Portal.
- Continued successful implementation of the Consequence-Based Top Screen (CTS) methodology to identify critical assets with a total of 372 assets entered into the CTS database as of June 2012.

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 the following:

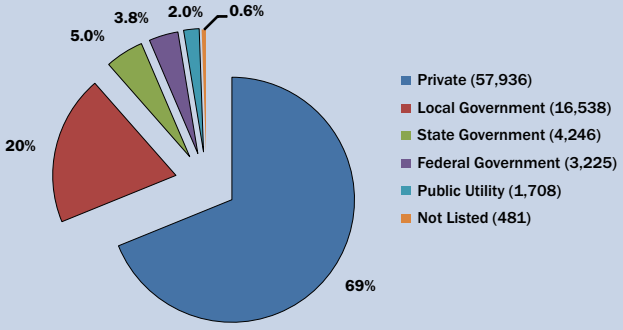
- Developing improved blast-induced damage analysis capabilities and simplified damage estimation models.
- Identifying and characterizing Dams Sector assets and providing a sector-wide prioritization framework.
- Assessing the economic and loss-of-life consequences of dam failures.
- Determining the status of State-level dam security and protection jurisdictional programs.
- Improving regional resilience and preparedness through an annual series of exercises.
- Developing and widely distributing technical reference handbooks, guides, and training materials.
- Developing guidance aimed at strengthening cybersecurity within the Dams Sector.
- Improving the communication between partners and Federal entities.

PATH FORWARD

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

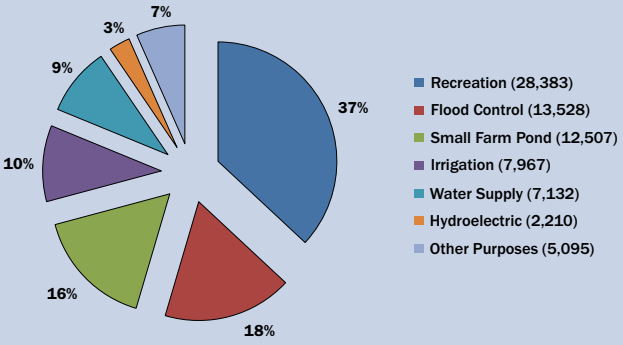
- Continue to safeguard facility-sensitive information from disclosure.
- Continue to identify and characterize critical assets in an effort to demonstrate the need for a risk-based, multiyear, and multijurisdictional infrastructure rehabilitation program.
- Increase reliance on HSIN–CS by enabling virtual participation in sector quarterly councils and workgroup meetings.

Dam Owners by Type

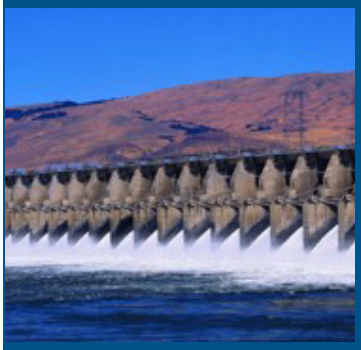


Source: National Inventory of Dams (2012)

Dams by Primary Purpose



Source: National Inventory of Dams (2012)



GCC MEMBERS

- Bonneville Power Administration
- Commonwealth of Pennsylvania, Department of Environmental Protection
- Federal Energy Regulatory Commission
- International Boundary & Water Commission
- New York City, Department of Environmental Protection
- 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
- 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

- Ameren Services Company
- American Electric Power
- Association of State Dam Safety Officials
- Association of State Floodplain Managers
- Avista Utilities
- BC Hydro
- Chelan County
- Colorado River Energy Distribution Association
- Consumers Energy
- Dominion Resources
- Exelon Corporation
- Hydro-Québec
- National Association of Flood & Stormwater Management Agencies
- National Hydropower Association
- National Mining Association
- National Water Resources Association
- New York Power Authority
- Ontario Power Generation
- Pacific Gas and 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
- United States Society of Dams
- Xcel Energy Corporation

25

DEFENSE INDUSTRIAL BASE SECTOR

PARTNERSHIP

The Defense Industrial Base (DIB) consists of domestic and foreign entities that research, develop, design, produce, deliver, and maintain military weapons systems, subsystems, components, and piece parts for the U.S. Department of Defense (DOD). The defense products and services provided by the DIB equip, inform, mobilize, deploy, and sustain forces conducting military operations worldwide.

The DIB Sector Government Coordinating Council (GCC) is composed of members from the DOD, U.S. Department of Commerce, U.S. Department of Energy, U.S. Department of Homeland Security, U.S. Department of Justice, U.S. Department of State, and U.S. Department of the Treasury. The DIB Sector Coordinating Council (SCC) is made up of members of defense industry associations and DIB private sector critical infrastructure owners and operators.

VISION

As the Sector-Specific Agency, the DOD is responsible for leading collaborative risk management activities aimed toward eliminating or mitigating unacceptable levels of risk to physical, human, and cyber infrastructure assets, systems, and networks. DIB activities support national security objectives, ensure public health and safety, and establish public confidence.

GOALS

The following sector goals were established in the 2010 Sector-Specific Plan and 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 (Cybersecurity/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 or high impact to critical infrastructure or DIB assets.

SELECTED ACCOMPLISHMENTS

Sector partners continue to 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 and prioritizing the criticality of private sector DIB assets and collaborated with the DIB SCC to improve the annual criticality determination process.
- Developed a self-assessment tool for small- and medium-sized companies to assess physical security.
- 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.
- Maintained an emergency notification system that can reach sector SCC partners.
- Converted the DIB Cybersecurity/Information Assurance Pilot to program status.

KEY INITIATIVES

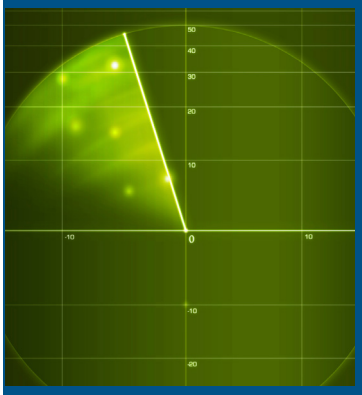
DOD collaborates with DIB asset owners and operators to develop plans to implement protection measures. Owners and operators make risk reduction decisions, but DOD strives to facilitate informed decision making by encouraging information sharing and making decision-support tools available. Key initiatives within the sector include the following:

- Conducting two regional energy dependency assessments and recommending a dependency analysis methodology that partners may use.
- Identifying existing information-sharing portals and pursuing a system that will enable a robust two-way classified information-sharing capability.
- Working to improve sector information sharing at the local level and to integrate owners and operators into information-sharing environments at State and major urban area fusion centers.

PATH FORWARD

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

- Continue the partnership-oriented approach to refine, develop, and implement strategies and program implementation plans vital 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.
- Focus annual activity on the set of shared objectives in the current *GCC/SCC Joint Business Plan*, which is based on the goals of the Sector-Specific Plan and on current trends or threats that impact the sector.



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
- Aerospace Industries Association
- Alliant Techsystems
- ASIS 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
- L3-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.
- TASC, Inc.
- Textron, 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 for 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 serves as the Sector-Specific Agency (SSA) for the ESS. The ESS SSA 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. The GCC assists in coordinating critical infrastructure strategies, activities, policies, and communications within Federal 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 the GCC. The SCC is organized through professional associations that represent the five emergency service disciplines: law enforcement, fire and rescue services, emergency management, emergency medical services, 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:

- Deployed the Web-based Emergency Services Self-Assessment Tool (ESSAT).
- Delivered a beta test of an exercise series specifically designed for first-responder chief officers and senior officials. The day-long event included full representation from the City and County of Denver's first-responder organizations, with more than 35 participants. The exercise broke ground as the first exercise to focus specifically on ESS resilience and continuity of operations.
- Led a continuity of operations and critical infrastructure resilience preparedness initiative for the City of Charlotte and Mecklenburg County in preparation for an upcoming National Special Security Event. The ESS hosted leadership meetings as well as continuity training and plan development workshops, and also developed a validation exercise. In all, more than 20 city and county departments were represented, with more than 100 public sector representatives participating.
- Distributed 1,000 First Responder Readiness Program informational packages through conferences and meetings.
- Registered 552 participants for the Ready Responder Program for the ESS Webinar and 140 participants for the Cybersecurity in the ESS Webinar.
- Jointly conducted a sector-wide Cyber Risk Assessment with the National Cybersecurity Division (NCSD) in order to provide a cybersecurity risk profile that ESS partners can use to enhance the security and resilience of ESS disciplines.
- Developed the *Roadmap to Secure Voice and Data Systems in the Emergency Services Sector*, a strategic resource and a path forward for sector partners looking to further develop their technology security.

- Integrated the newly formed SCC Credentialing & Disaster Reentry Working Group (CDRWG) into Federal policy and technology initiatives addressing first-responder credentialing. As a result, the CDRWG influenced Federal credentialing policy and improved internal reports that create methodologies 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, thereby protecting the capacity of the ESS.
- Introduced new thinking that altered the outcomes of a multisector DHS risk study identifying interdependent vulnerabilities between the ESS and the Communications Sector.

KEY INITIATIVES

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

- Establishing a Sector Initiatives Call to capture numerous activities impacting the ESS; these activities are communicated to the sector at regularly scheduled SCC and GCC meetings.
- Identifying and managing risk through DHS field facility security initiatives, such as Site Assistance Visits, the Buffer Zone Protection Program, and Enhanced Critical Infrastructure Protection assessments.
- Improving the sharing of timely, validated, protected, and actionable information that is supported by extensive education, training, and awareness programs through the ESS Information Sharing Working Group and the Homeland Security Information Network-ESS Community of Interest.
- 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 National Level Exercise 2012 and the Denver Interagency Continuity of Operations Exercise.
- Participating in NCSD's 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 systems, 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.

PATH FORWARD

To address future challenges, the sector will pursue the following activities:

- Continue to work collaboratively with NCSD throughout 2012 on various cybersecurity initiatives, such as distribution of the Cyber Risk Assessment, further development of the ESS Cyber Roadmap, and information-sharing efforts as necessary.

GCC MEMBERS

- National Voluntary Organizations Active in Disaster
- 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 Transportation
- U.S. Environmental Protection Agency

SCC MEMBERS

- American Ambulance Association
- American Public Works Association
- Central Station Alarm Association
- Electronic Security Association
- International Association of Chiefs of Police
- International Association of Emergency Managers
- International Association of Fire Chiefs
- Mississippi Rural Water Association
- National Association of Security Companies
- National Association of State EMS Officials
- National Emergency Management Association
- National Fire Protection Association
- National Native American Law Enforcement Association
- National Pegasus Program
- National Sheriffs' Association
- New York City Fire Department
- North County Fire Protection District, Winchester, Virginia
- Rescobie Associates, Inc.
- Securitas Security Services
- Security Industry Association
- Story County, Iowa Sheriff's Office

- Promote cybersecurity awareness and information sharing about sector-specific threats.
- 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, as well as develop outcome metrics through the ESSAT program.
- Market the Resilience Development Program, which will consist of infrastructure protection products and expertise. It will be offered to ESS practitioner organizations with the intent of providing customized enhancements to their resilience and overall readiness.
- 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 of which were 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.

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, and regulated by numerous public and private owners and operators. The sector's public-private partnership facilitates information sharing regarding threats, vulnerabilities, and protective measures. Private sector partners are represented by two Sector Coordinating Councils (SCCs), the Electricity SCC and the Oil and Natural Gas SCC, which essentially represent all sector asset owners and operators. Public sector partners with interests in the Energy Sector compose the Energy Sector Government Coordinating Council (GCC), and the U.S. Department of Energy (DOE) serves as chair of the council and 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 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 goals:

- Establish robust situational awareness within the Energy Sector through timely, reliable, and secure information exchanges among trusted public and private sector 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.
- Define critical infrastructure protection roles and responsibilities among all Federal, State, local, and private sector partners and work to create efficiency and improved coordination throughout the partnership.
- Understand key sector interdependencies and work to evaluate and address them by incorporating that understanding 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 programs and processes.

SELECTED ACCOMPLISHMENTS

Sector partners continue to maintain and enhance the reliability and resilience 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 Subsector that were aligned with the goals of the Transportation Security Administration pipeline modal SSA and updated the *2011 Oil and Natural Gas Sector Coordinating Council Strategic Plan*.
- Developed Electricity Subsector performance metrics aimed to inform, increase transparency of, and quantify the effectiveness of risk reduction and mitigation actions, illustrating the North American Electric Reliability Corporation's (NERC) reliability performance results and trends.
- Made significant progress in the development of sector-specific metrics in the Electricity Subsector and the Oil and Natural Gas Subsector.
- Released the revised Energy GCC Charter, with added goals and responsibilities.
- Finalized and published updates to strategic plans, including the *Roadmap to Secure Control Systems in the Energy Sector* and the *Roadmap to Achieve Energy Delivery Systems Cybersecurity*.
- Delivered or expected to deliver final reports by four of NERC's major task forces that provide guidance and options to enhance the resilience of the bulk power system to withstand and recover from events and improve the Electricity Subsector's reliability and resilience.
- Released its first annual *State of Reliability Report*, in which NERC reviews and assesses the state of reliability based on metrics trends and provides an integrated view of reliability performance.
- Established the National Electric Sector Cybersecurity Organization.
- Conducted the first annual Grid Security Exercise in November 2011, which involved more than 250 participants and tested NERC's and the electricity industry's crisis response plans and validated current readiness in response to a cyber incident.
- Hosted the 2011 Grid Security Conference, which is part of NERC's ongoing security awareness program and is designed to bring together industry and government security professionals to discuss grid cybersecurity concerns as well as trends and best practices in security throughout the industry.
- Developed and published the *Electricity Subsector Cybersecurity Risk Management Process* guidelines through the collaborative efforts of DOE, the National Institute of Standards and Technology, and NERC. The guidelines are designed to help utilities better understand cybersecurity risks, assess severity, and allocate resources more efficiently to manage cybersecurity risks.

KEY INITIATIVES

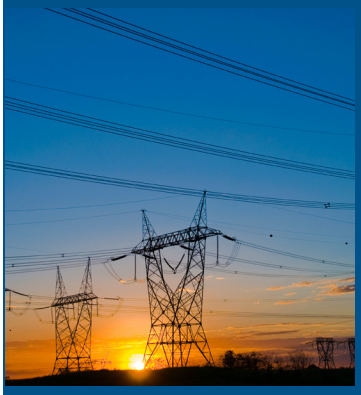
The Energy Sector is continuing to implement the following programs, which range from participating in cybersecurity and Smart Grid initiatives to studying the importance of hydroelectric power generation to the national economy and overall energy reliability:

- Developing and transferring risk assessment methodologies, such as the Enhanced Critical Infrastructure Protection assessments, which help identify vulnerabilities and enhance security through collaboration with Federal, State, local, and private sector stakeholders.
- Meeting regularly at the Assistant Secretary level with DOE, the U.S. Department of Homeland Security, and other agencies to share approaches and implement security practices related to energy system reliability, survivability, and resilience.
- Employing the Electricity Sector Cybersecurity Risk Management Maturity project, a White House initiative to develop a common risk-based model designed to help the Electricity Subsector evaluate its cybersecurity capabilities in a consistent manner, communicate capability levels in meaningful terms, and guide an organization in prioritizing cybersecurity investments.

PATH FORWARD

Although significant progress has been made in securing 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; training and exercises; energy situation reports; and the *National Electric Sector Cybersecurity Organization Resource.*



GCC MEMBERS

- Executive Office of the President
- Federal Deposit Insurance Corporation
- Federal Energy Regulatory Commission
- National Association of Regulatory Utility Commissioners
- National Association of State Energy Officials
- National Resources Canada
- U.S. Army Corps of Engineers
- U.S. Commodity Futures Trading Commission
- 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 Council
- Orlando Utilities Commission
- Sho-Me Power Electric Cooperative
- UIL Holdings Corporation

OIL AND NATURAL GAS SCC MEMBERS

- American Exploration & Production Council
- American Fuel and Petrochemical Manufacturers
- American Gas Association
- American Petroleum Institute
- American Public Gas Association
- Association of Oil Pipe Lines
- Canadian Association of Petroleum Producers
- Canadian Energy Pipeline Association
- Energy Security Council
- Gas Processors Association
- Independent Petroleum Association of America
- International Liquid Terminals Association
- Interstate Natural Gas Association of America
- National Association of Convenience Stores
- National Ocean Industries 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). The USDA is responsible for production agriculture and food, which includes meat; poultry; and frozen, liquid, and dried egg products. The 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 decision making 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:

- Participated in a series of facilitated meetings and conference calls among the FA Sector GCC's 21 member organizations that resulted in the development of the *Strategic Plan 2011*.
- Released the *Strategic Plan 2011* that outlines three years of risk reduction activities and enables Council members to work closely with industry partners to share information and jointly pursue tools, programs, and activities that support private sector security efforts.
- Developed the *Value Proposition and Engagement Plan* and the *Implementation Plan for Enhancing the Public-Private Partnership* that aim to improve awareness and engagement on FA Sector issues.
- Launched tools to help owners and operators identify mitigation strategies and preventive measures.
- 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.

KEY INITIATIVES

Key initiatives within the FA Sector include the following:

- Improving the visibility and awareness of the sector through strategic planning efforts.
- Maintaining and improving mechanisms for robust intra-GCC collaboration and coordination through partnership activities with interdependent sector partners.
- Expanding State, local, tribal, and territorial participation and leadership within the FA Sector GCC.
- Facilitating information sharing, best practices, and outreach efforts through the development and dissemination of education and orientation materials for new FA Sector GCC members.
- Refining and enhancing information-sharing, collaboration, and communications processes that include regular newsletters and use of the Homeland Security Information Network—Food and Agriculture portal and FoodSHIELD.
- Leveraging available technology and Web tools to deliver FA Sector GCC news, resources, and information to a wide public and private sector audience.
- Promoting and using research capabilities, sector knowledge, and existing tools and programs to strengthen sector resilience.
- Implementing a three-year exercise and training calendar.
- Continuing and expanding use of the Food and Agriculture Sector Criticality Assessment Tool.
- Identifying meaningful metrics to gauge sector progress and compile and disseminate success stories, case studies, best practices, and lessons learned to sector partners.

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. Through its partnership and engagement on FA Sector issues, the FA Sector will take numerous additional steps to move forward, including the following:

- 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.

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
- Bunge North America
- 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
- 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

SCC MEMBERS CONTINUED

- Keystone Foods
- Kraft Foods Global, Inc.
- The Kroger Company
- Land O'Lakes, Inc.
- Marriott International
- McCormick & Company, Inc.
- Milkco, Inc.
- MillerCoors LLC
- National Association of Convenience Stores
- National Association of Wheat Growers
- 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 Council
- National Renderers Association
- National Restaurant Association
- National Retail Federation
- North American Millers' Association
- PepsiCo, Inc.
- Publix Super Markets, Inc.
- Quaker Oats
- Sara Lee Corporation
- Snack Food Association
- Star of the West Milling Company
- The Sugar Association
- Super Store Industry/Turlock Dairy Division
- Tuna Council
- Tyson Foods, Inc.
- United Fresh Produce Association
- USA Rice Federation

33

GOVERNMENT FACILITIES SECTOR

PARTNERSHIP

The Government Facilities Sector (GFS) includes a wide variety of facilities located both in the United States and overseas that are owned or leased by Federal, State, local, tribal, or territorial governments. 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, the GFS covers 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 includes representatives from government entities responsible for the protection of government facilities. FPS is engaging with the GCC, the General Services Administration, and the Interagency Security Committee (ISC) to develop an action plan that identifies cross-cutting issue for the sector while capitalizing on existing partnerships and coordination mechanisms among stakeholders, to more closely focus the strategic needs of the sector, and to allow for more active coordination among subsector partners.

The GFS also includes the Education Facilities Subsector (EFS), which consists of all prekindergarten through higher education public, private, and proprietary education facilities. This subsector faces some unique challenges as it includes both government- and private sector-owned facilities. All subsector critical infrastructure protective efforts are designed to support the overall EFS vision that all education facilities are ready to prevent, mitigate, prepare for, respond to, and recover from any natural or manmade hazard by having a comprehensive all-hazards plan to enhance safety, minimize disruption, and ensure the continuity of the learning environment.

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.

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.
- Produced the Federal Facility Threat Picture, a quarterly threat assessment focusing on threats posed by international terrorism, domestic extremists, lone offenders, and criminal organizations who may seek to attack or exploit elements of the sector.

KEY INITIATIVES

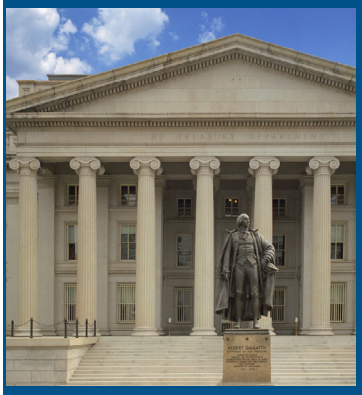
FPS and its partners are already implementing numerous protective programs that meet GFS goals and are contributing to a more secure sector. These protective programs range from visual situational awareness at major public events to continuity of operations planning. Key initiatives within the sector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

- 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 ISC'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 U.S. Office of Personnel Management's Electronic Questionnaires for Investigations Processing system to conduct background investigations.
- Maintaining and/or revising Occupant Emergency Plans.
- Sustaining public safety through the Crime Prevention and Awareness program.
- Monitoring and promoting the implementation of key Federal information security initiatives.

PATH FORWARD

Numerous steps will be taken as the 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 and other IT infrastructure, including database integration.
- Continue to manage communications with internal and external partners and implement design and change management strategies to ensure that sector 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.



GCC MEMBERS

- Administrative Office of the United States Courts
- City of Fort Worth, Texas
- City of Las Vegas, Nevada
- Federal Reserve Board
- General Services Administration
- Michigan State Police
- National Academy of Sciences
- National Air and Space Administration
- National Archives and Records Administration
- Social Security Administration
- State of New York, Division of Homeland Security and Emergency Management
- U.S. Department of Agriculture
- 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 State
- U.S. Department of the Treasury
- U.S. Department of Transportation
- U.S. Department of Veterans Affairs
- U.S. Environmental Protection Agency
- U.S. Office of Personnel Management

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 owner and operator 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 collaboratively 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 the workforce's health and safety and limit its ability to carry out its 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:

- Implemented the Critical Asset Identification Process (CAIP), in which the HPH Critical Infrastructure Protection (CIP) Program collaborates with SCC subsector leadership, subject matter experts, and relevant critical infrastructure owners and operators to nominate a list of critical assets. The HPH Sector nominated nationally critical assets (Level 1, Level 2, and Level 3) in 2011, and it will focus on regional, State, and local assets (Level 4 and Level 5) in 2012.
- Designed 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 (DHS) Office of Health Affairs.
- Began preparing a new Webinar series that will help educate HPH Sector partners on a variety of topics related to HPH Sector critical infrastructure protection.
- Increased the combined membership of the Homeland Security Information Network (HSIN)–HPH portal over the course of the 2012 reporting period through HPH Sector trade association outreach, dissemination of HSIN portal marketing materials, and the new Webinar series, enabling the sector to provide threat and risk information to hundreds more sector stakeholders.
- Utilized HSIN–HPH as an information-sharing portal during the response to Hurricane Irene in August 2011, which enabled the HPH CIP Program to populate an incident site with incident-specific information, mapping products that highlighted potential impacts to infrastructure of concern, and a discussion board for HPH Sector partners to share information.
- Held meetings with four joint working groups dedicated to a variety of topics (Cybersecurity, Information Sharing, Research and Development, and Risk Management) and made up of HPH Sector subject matter experts to develop new ideas and products that provide specific benefits to the sector, including (1) a primer providing introductory information on cybersecurity tailored specifically to the HPH Sector, (2) a brochure highlighting best practices on managing water usage during a water service interruption to HPH Sector facilities, and (3) informational fact sheets on the CIP Program and the goals and objectives of each of the HPH Sector working groups.

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 the following:

- Conducting four classified briefings per year for those stakeholders in the partnership who possess a Secret–level clearance or higher, conducting unclassified briefings based on redacted information with larger audiences, and presenting at various sector conferences to inform attendees about the CIP Program and a variety of topics related to critical infrastructure protection.
- Funding security clearances for State health department personnel, including State health officials and directors of public health preparedness (three per State).
- Continuing efforts to improve the HSIN–HPH portal to make it a repository for timely and actionable information for the sector related to steady-state and emergency response scenarios.
- Disseminating a biweekly newsletter to all users highlighting HPH and articles and reports focused on critical infrastructure protection added to the HSIN–HPH portal document library.
- Working with manufacturers of drugs, biological products, and medical devices 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.
- Collaborating with the U.S. Department of Energy to implement the Power Monitoring Pilot Program, which will install devices in critical HPH facilities throughout the Nation to constantly monitor and provide real-time communication on the facilities' power status.
- Developing a Liaison Officer Program in which members of the private sector and State and local partners could be engaged and assist

with responding and manning the HHS Secretary's Operations Center during an all-hazards event.

- Working with internal and external agencies and organizations on cybersecurity initiatives and products.
- 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.
- Collaborate with HPH Sector partners to strengthen communication and engagement during both steady state and incident response.
- Coordinate outreach and information sharing with facilities identified through CAIP with DHS and other Federal, State, and local partners.

GCC MEMBERS

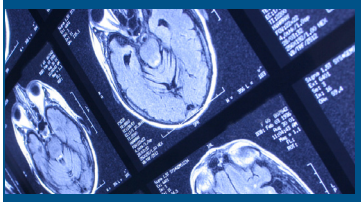
- Association of State and Territorial Health Officials
- National Association of County and City Health Officials
- National Indian Health Board
- Southern Nevada Health District
- State of Maryland, Department of Health
- State of Michigan, Department of Health
- State of Virginia, Department of Health
- State of Washington, Department of Health
- 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

SCC MEMBERS CONTINUED

- American Association of Occupational Health Nurses
- American Association of Poison Control Centers
- American Association of Tissue Banks
- American College of Emergency Physicians
- American College of Occupational and Environmental Medicine
- American College of Physicians
- American Healthcare Association
- American Hospital Association
- American Industrial Hygiene Association
- American Medical Association
- American Medical Depot
- American Nurses Association
- American Osteopathic Association
- American Red Cross
- American Society of Health Systems Pharmacists
- America's Health Insurance Plans
- Amgen Inc.
- Archdiocese of Washington
- Association of Healthcare Resource and Materials Management Professionals
- Association of Public Health Laboratories
- Baxter Healthcare Corporation
- Baylor Healthcare System
- Biotechnology Industry Organization
- Blood Centers of America



SCC MEMBERS CONTINUED

- Blue Cross and Blue Shield of Florida
- Blue Shield of California
- BLU-MED Response Systems
- Brooklawn Memorial Park
- Business Continuity Consulting
- Cardinal Health
- Carolinas Healthcare System
- Casket and Funeral Supply Association
- Catholic Cemetery Conference
- Control Risk/RX Response
- Cremation Association of North America
- Dartmouth Hitchcock Medical Center
- Dodge Company
- Generic Pharmaceutical Association
- Genzyme Corporation
- The George Washington University Medical Center
- Greater New York Hospital Association
- Group Health Cooperative
- Hanover Hospital
- Health Industry Distributors Association
- Health Information and Management Systems Society
- Health Promotion Consultants
- Healthcare Distribution Management Association
- Henry Schein
- Hospital Association of Southern California
- Humana
- Independence Blue Cross
- Inova Health System
- International Association for Healthcare Security & Safety
- International Cemetery, Cremation, and Funeral Association
- James B. Haggin Memorial Hospital
- Johns Hopkins University
- Johnson Memorial Medical Center
- The Joint Commission
- Kaiser Permanente
- Laboratory Corporation of America

SCC MEMBERS CONTINUED

- Lafayette General Medical Center
- Lincoln-Lancaster County, Nebraska
- Mary Washington Healthcare
- Matthews Cremation
- McAfee
- Medco Health Solutions, Inc.
- Medline Industries, Inc.
- Memorial Sloan Kettering Cancer Center
- Merck & Co., Inc.
- Monmouth Ocean Hospital Service Corporation
- Mount Sinai and 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 Health Information Sharing & Analysis Center
- The Nemours Foundation
- Nevada Hospital Association
- Operation PAR, Inc.
- Owens & Minor, Inc.
- Pharmaceutical Research and Manufacturers of America
- The Regence Group
- Regional Medical Center
- Samaritan Health Services
- Siemens Healthcare USA
- SMA Technology Group
- The Tauri Group
- Terumo Medical Corporation
- Texas A&M University
- Tronex International, Inc.
- Tuomey Healthcare System
- Universal Hospital Services
- University of California, Los Angeles Medical Center
- University of Montana
- University of Pittsburgh Medical Center
- Verizon
- Virginia Hospital & Healthcare Association
- Washington Occupational Health Associates, Inc.
- WellPoint, Inc.

37

INFORMATION TECHNOLOGY SECTOR

PARTNERSHIP

The Information Technology (IT) Sector produces and provides high-assurance IT products and services for governments, critical infrastructure sectors, commercial businesses, and private citizens around the globe. 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. The IT Sector Coordinating Council (SCC) consists of private sector partners who work alongside their public sector counterparts in the Government Coordinating Council (GCC). The Office of Cybersecurity and Communications, within the U.S. Department of Homeland Security (DHS) National Protection and Programs Directorate, serves as the IT Sector-Specific Agency. As Co-Chair of the Cross-Sector Cybersecurity Working Group (CSCSWG), the IT Sector provides leadership on the cybersecurity mission by prioritizing topics for discussion and supporting targeted cybersecurity activities within the CSCSWG.

VISION

The IT Sector's vision is a secure, resilient infrastructure, achieved by 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:

- **Proactive Prevention and Protection through Risk Management**: Identify, assess, and manage risks to the IT Sector's critical functions and international dependencies.
- **Enhanced 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 to appropriately equip stakeholders to identify and effectively respond to incidents that do occur.
- **Effective 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 Improvements**: 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:

- Identified key risks and recommendations to manage those risks, and identified gaps that need to be addressed to enhance identity management across the ecosystem in the IT Sector Identity Management and Associated Trust Support Services Risk Assessment. Announced the risk assessment at the National Institute of Standards and Technology (NIST) ID Trust Conference as part of a panel discussion to help inform implementation of the *National Strategy for Trusted Identities in Cyberspace (NSTIC)*.
- Updated the analysis of risks to Domain Name Resolution Services (DNS) infrastructure by considering changes since the release of the *Provide Domain Name Resolution Services* critical function risk profile in the 2009 baseline *IT Sector Risk Assessment (ITSRA)* and seeking to understand and helping to manage new and emerging risks resulting from technological changes and evolving strategic and operational threats.
- Identified and examined areas for improvement in incident response policy and operations by contributing to and participating in Cyber Storm IV and National Level Exercise 2012, which simulated response to national-level cybersecurity incidents.
- Provided constructive feedback on priority areas associated with the DHS Cyber Ecosystem framework and ensuing *Blueprint for a Secure Cyber Future* strategy.
- Shared information, priorities, and experiences through monthly and ad hoc working groups to better coordinate government and industry efforts and to share expertise and best practices.

KEY INITIATIVES

Key initiatives within the IT Sector include:

- Coordinating across critical infrastructure sectors on situational awareness and response and recovery activities through the IT Information Sharing and Analysis Center and United States Computer Emergency Readiness Team.
- Engaging in risk assessment and risk management activities across the sector's critical functions to catalogue risks to the sector's infrastructure, identify management activities in response to those risks, and update the sector's risk profile.
- Promoting voluntary efforts to reduce the impact of botnets in cyberspace and sharing practices for preventing and detecting infections, understanding notifications, and remediating devices and recovering through involvement in the Internet Botnet Group.
- Facilitating progress towards an identity ecosystem by participating in the NSTIC's implementation efforts and pilot programs, and highlighting key risks and recommended mechanisms to address them.

- Advancing collaboration among the Federal Government, international organizations, and the private sector on cybersecurity, including providing input into policy formulation (e.g., *International Strategy for Cyberspace*) and processes to reflect alignment with IT Sector interests and priorities; providing subject matter expertise on committees and working groups (e.g., United States-European Union Working Group on Cybersecurity and Cybercrime); and participating in key events (e.g., Internet Governance Forum, International Telecommunication Union World Conference on International Telecommunications).
- Working to ensure supply chain risks are effectively managed by documenting and sharing supply chain risk management practices through multiple forums and initiatives, including NIST's Draft NIST Interagency Report 7622 *Supply Chain Risk Management Practices for Federal Information Systems.*
- Providing proper and consistent cyber security training, workforce development, and education, at both the national and organizational levels, through participation in efforts such as the National Initiative for Cybersecurity Education.

PATH FORWARD

Effective collaboration between the public and private sectors has driven significant progress in the past. For example, the baseline ITSRA and associated risk management strategies (e.g., *IT Sector Risk Management*) helped government and industry to better understand and manage risks to the IT Sector's critical functions, and represented the result of unprecedented partnership and collaboration. More recent work on the IT Sector Identity Management and Associated Trust Support Services Risk Assessment and the update to the IT Sector DNS Risk Profile are similarly founded on partnerships, shared commitment, and shared expertise. Throughout 2012 and 2013, IT Sector partners will seek to reenergize the partnership between public and private sectors through the following activities:

- Initiate collaborative planning to identify shared goals and objectives and work to coordinate more effectively.
- Continue advancing key initiatives through performing and engaging in initiatives and activities consistent with the sector's goals, including those related to information sharing, risk management, international collaboration, and education and awareness; conducting strategic, outcome-focused risk analyses and recommending actions for government and industry; and improving operational coordination, including by sharing information and participating in exercises.
- Build on and amplify the impact of work, including by enhancing reach, increasing visibility, and broadening awareness of the relevance and value of sector work products in complementing and expanding on existing Federal Government and industry efforts.

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
- CA Technologies
- Center for Internet Security
- Certichron Inc
- Cisco Systems, Inc.
- Coal Fire Systems
- Computer and Communications Industry Association
- Computer Sciences Corporation
- Computing Technology Industry Association
- Concert Technologies
- Core Security Technologies
- Cyber Pack Ventures Inc.
- Cyber Security Industry Alliance
- Dell
- Deloitte & Touche LLP
- Detica
- Dynetics, Inc.
- Ebay
- Echelon One
- Electronic Industries Alliance
- EMC Corporation
- Entrust, Inc.
- Equifax, Inc.
- EWA Information & Infrastructure Technologies, Inc.
- The Experts, Inc.
- General Atomics
- General Dynamics
- Google
- Green Hills Software
- Hatha Systems
- HP
- IBM Corporation
- Information Systems Security Association
- Information Technology Industry Council
- Information Technology - Information Sharing & Analysis Center
- Intel Corporation
- International Security Trust and Privacy Alliance
- International Systems Security Engineering Association
- Internet Security Alliance

SCC MEMBERS CONTINUED

- ITT Exelis
- Juniper Networks
- KPMG LLP
- L-3 Communications
- Lancope, Inc
- Litmus Logic
- LGS Innovations
- Lockheed Martin
- Lumeta Corporation
- Lunar Line
- McAfee
- 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
- Secure Computing
- Sentar Inc
- Serco
- Siemens Healthcare
- The SI Organization
- 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

39

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. Federal Government. However, based on their primary purposes, some physical structures considered monuments or icons (e.g., the Golden Gate Bridge, Hoover Dam, and the U.S. Capitol Building) have been assigned to other sectors, such as Transportation Systems, Commercial Facilities, Dams, and Government 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 serves as the Sector-Specific Agency for the NMI Sector and 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. As 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 of NMI Sector assets.
- Maintain rapid and robust information sharing and communications between intelligence and law enforcement agencies and Government Coordinating Council (GCC) partners that operate sector assets.
- Integrate robust security, technology, and protection 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.
- Review and update security programs to adjust to seasonal and event-specific security challenges.

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 of three sector assets and encouraged sector partners to perform independent assessments and update protective systems.
- Worked extensively with the U.S. Department of Homeland Security (DHS) National Cybersecurity Division and held three cyber 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 identified needs and gaps in plans, programs, policies, procedures, and strategies.
- Replaced explosive trace detection units and metal detection equipment at the Washington Monument.
- Provided funding for maintenance of the National Mall cameras.
- Made progress in the construction of hardened security barriers at multiple national museums.
- Continued the Community Anti-Terrorism Training Institute's C.A.T. 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.
- The National Park Service U.S. Park Police (USPP) established a Tactical Technology Deployment Program, which leverages wireless capabilities to bring a rapidly deployable, real-time situational awareness to events and incidents.

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 the following:

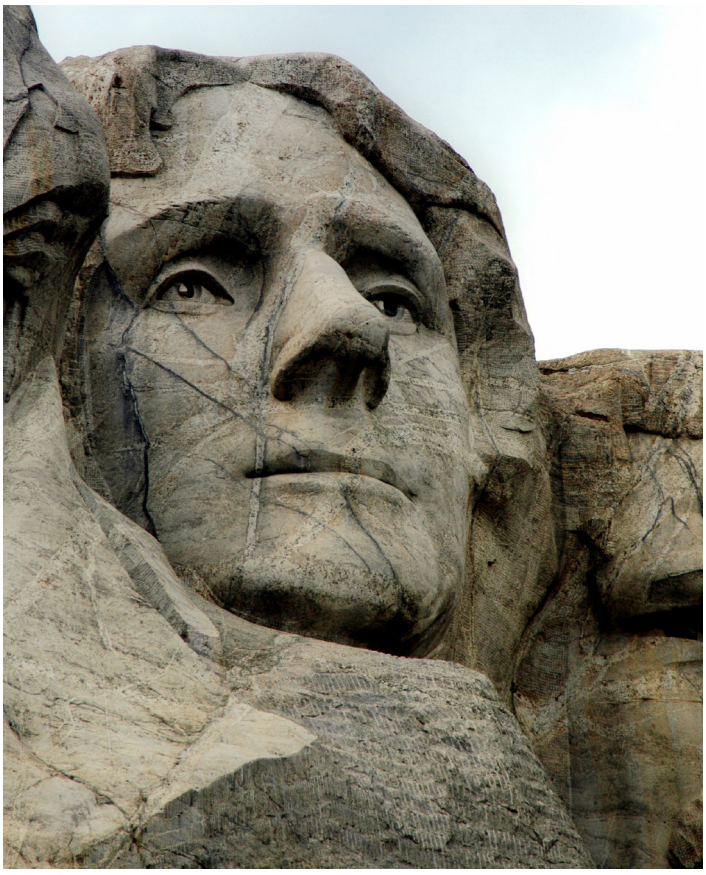
- Funding additional commissioned law enforcement and contract security personnel positions to sustain 360-degree security coverage and maintain staffing for other mission requirements.
- Developing unobtrusive physical security techniques and/or environmental/architectural designs that enhance perimeter security; cost-effective visitor screening technology that maintains accessibility/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 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 and other security-related initiatives, such as the Lower Manhattan Protection Zone.
- Partnering with a private sector donor to replace the aging closed-circuit television system at the Statue of Liberty.
- Participating through USPP, a principal partner in the National Capital Region's (NCR) Preventative Radiological Nuclear Detection initiative, which seeks to integrate detection equipment within the NCR to support the homeland security mission.
- Working with DHS on a formal "See Something, Say Something"™ campaign that will focus on public education, signage, and reporting procedures.

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, a park key system, a 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.



GCC MEMBERS

- National Archives and Records Administration
- Smithsonian Institution
- U.S. Capitol Police
- U.S. Department of Defense
- 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 (SCC) and the Nuclear Government Coordinating Council (GCC) 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 supports 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 the 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 hazards 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 the Integrated Comprehensive Exercises at Davis Besse Nuclear Power Station.
- Installed voluntary security enhancements developed by the National Nuclear Security Administration (NNSA) at three non-power reactors in Fiscal Year (FY) 2011.
- Recovered more than 30,200 disused radioactive sources (more than 828,000 curie) since 1997, including 2,571 sources in FY 2011.
- Implemented security enhancements at 366 U.S. buildings with high-priority radiological materials through the NNSA as of April 30, 2012.
- 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 331 irradiators have received a retrofit kit. NNSA has been working with 60–80 volunteers per calendar year to implement the enhancements, and the two largest irradiator manufacturers have agreed to include the delay kits on newly produced units.

KEY INITIATIVES

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 the following:

- Implementing additional voluntary security enhancements, such as the Research and Test Reactors Voluntary Security Enhancement Project, Radiological Site Voluntary Security Enhancement Project, and Cesium Chloride Irradiator In-Device Delay Program.
- Conducting Integrated Pilot Comprehensive Exercises 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 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 implementation of the *Roadmap for Enhancing Cyber Systems Security in the Nuclear Sector*.
- 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 caused 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.

GCC MEMBERS

- Commonwealth of Massachusetts, Department of Public Health
- Commonwealth of Pennsylvania, Department of Environmental Protection
- Conference of Radiation Control Program Directors, Inc.
- Nuclear Regulatory Commission
- State of Delaware, Office of Radiation Control, Delaware Division of Public Health
- State of Florida, Department of Public 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 Company
- Covidien
- Dominion Generation
- Edison Electric Institute
- Edlow International Company
- Entergy Operations
- Exelon Generation Company, LLC
- General Electric Hitachi
- Michigan State University
- Nuclear Energy Institute
- Oregon State University
- Purdue University
- QSA-Global
- Rutgers University
- Security Engineering Associates
- Southern Nuclear Operating Company
- 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 employs 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.

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 the law enforcement and intelligence communities to facilitate a better understanding of the information requirements of the P&S Sector.
- Ensure timely, relevant, and accurate threat reporting from the law enforcement and intelligence communities to key decisionmakers in the sector in order to implement appropriate threat-based security measures and risk management programs.
- Develop cross-sector coordination mechanisms to identify key interdependencies, share operational concerns, and develop protective protocols with the Commercial Facilities, Communications, Energy, Healthcare and Public Health, Information Technology, and Transportation Systems 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, radiological, or nuclear 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, as well as to 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:

- 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 two Critical Infrastructure Partnership Advisory Council meetings.
- Reviewed the status of sector programs and GCC structure and membership to make recommendations for strengthening the GCC charter.
- Conducted outreach to sector components not represented on the SCC.
- Responded to dozens of emergencies related to hurricanes, floods, fires, and other incidents.

KEY INITIATIVES

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

- Enhancing cybersecurity awareness.
- Targeting high-value cyber crimes.
- Mitigating risks to new postal products and business planning.
- Enhancing frontline employee awareness.
- Identifying cross-sector risks.
- Improving sector resilience.
- Identifying supply chain vulnerabilities.
- Identifying integrated carrier vulnerabilities.
- Strengthening supply chain security awareness.
- Establishing and implementing global security protocols for international mail.
- Participating in tabletop exercises and full-scale exercises at P&S facilities nationwide, including National Level Exercise 2012 and Cyber Storm III.

- Supporting and participating in the sector's Cities Readiness Initiative.
- Enhancing emergency preparedness.
- Facilitating the sharing of security information.

PATH FORWARD

The P&S Sector faces international and domestic threats that involve exploiting the sector's access to reach potential 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 address these challenges the sector will pursue the following activities:

- 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 and foster communication channels to support 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 for engagement.
- 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.
- Test resilience and recovery capabilities 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.

GCC MEMBERS

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

SCC MEMBERS

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

45

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 SCCs and/or GCCs for five of the six 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 venues 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 leveraged for collaboration, cooperation, and communication, when appropriate. The State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) also strengthens sector partnerships as it brings together experts from a wide range of professional disciplines related to critical infrastructure protection and resilience. 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 related to 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 on 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, including the following:

- Implemented risk-based security enhancements at airports, including TSA Pre✓™, to focus on high-risk screening and expedited travel for those considered to be a lesser risk.
- Reviewed airport regulations, resulting in improved airport security programs.
- Distributed a compendium of best practices to 446 commercial airports.
- Expanded collaborative infrastructure security coverage through thousands of Visible Intermodal Prevention and Response team deployments.
- Implemented enhanced screening measures and new procedures, including the Secure Flight watch list matching program, Certified Cargo Screening Program, and Next Generation Air Transportation System.
- Conducted, during Calendar Year 2011 (CY 2011), more than 160 surface mode assessments to inform risk reduction decisions.
- Reduced Toxic Inhalation Hazard cargo risks by more than 96 percent for high-threat urban areas since the 2006 baseline was released.
- Produced and distributed Transit and Rail Intelligence Awareness Daily reports to more than 2,000 public and private stakeholders through the Public Transportation and Surface Transportation Information Sharing and Analysis Centers.
- Partnered with maritime authorities in 150 foreign maritime authorities countries that conduct maritime trade with the U.S. to assess compliance with international anti-terrorism requirements and verify that effective anti-terrorism measures are implemented in foreign ports through the International Port Security Program.
- Completed, during CY 2011, 15 voluntary pipeline Corporate Security Reviews through joint public-private collaboration.
- Screened, during Fiscal Year 2011, over 472,000 vessels, including 122,000 commercial vessels, and 28 million crew members and passengers prior to arrival in U.S. ports.
- Enhanced risk-based decisionmaking through the Maritime Security Risk Analysis Model (MSRAM) to encourage asset-specific and area-wide security measures and response capabilities.
- Issued Security Awareness Messages recommending threat-specific protective measures to prevent and deter terrorist events.
- Enhanced preparedness, strengthened coordination, and shared security best practices and protective measures through regular teleconferences and meetings with senior security leaders of the 20 largest U.S. transit systems.
- Developed the *Transportation Systems Sector Cybersecurity Strategy* through the efforts of a joint sector working group.

KEY INITIATIVES

The Transportation Systems Sector is undertaking a variety of initiatives to enhance its protection and resilience. Several of these initiatives involve the modal GCCs bringing together numerous government agencies to collaborate on security efforts. Key initiatives within the sector include the following:

- Screening and vetting transportation workers through the Transportation Worker Identification Credential initiative and Hazmat Threat Assessment Program.
- Expanding intelligence-driven, risk-based initiatives in all modes.
- Securing critical physical infrastructure through the National Tunnel Security Initiative, general aviation security measurements, and Area Maritime Security Plans.
- Reducing freight rail risks using GPS technology on Toxic Inhalation Hazard cargo shipments.
- Leveraging technologies to screen travelers through Secure Flight and the deployment of checkpoint screening technologies.
- 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 Critical Rail Infrastructure 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.
- Using the Commercial Airports Risk Assessment Tool to help stakeholders make risk-informed resource allocation decisions.
- Developing a comprehensive strategic approach for identifying and managing cybersecurity risks to critical infrastructure operations.
- Continuing to implement the 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.
- Developing and releasing best practices to promote innovative and proven security measures.

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 sector and transportation owners and operators in strategic partnerships to develop efficient and effective security solutions.
- Collaborate with sector owners and operators to increase cybersecurity awareness and understanding and encourage the use of tools, audits, and assessments.
- Engage the SLTTGCC in risk management planning and programming processes.
- 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.
- Continue to encourage the intelligence community to efficiently provide reliable intelligence to the transportation community.
- Enhance international collaboration and supply chain security through engagement with foreign partners to increase the use of risk-based approaches.
- Work with the U.S. Department of State to effectively integrate and align critical infrastructure protection and resilience objectives with overall U.S. foreign policy.
- Promote awareness and education opportunities for critical infrastructure protection and resilience.
- Continue SLTTGCC engagement and information sharing.
- Publish rules to require certain owners and operators engaged in surface transportation to provide security training to frontline employees.
- Conduct periodic sector-wide risk assessments, including cyber-system assessments.
- Develop sector performance outcomes and metrics.

47

TRANSPORTATION SYSTEMS SECTOR

GCC MEMBERS

- American Association of State Highway and Transportation Officials
- Federal Energy Regulation 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
- Airlines for America
- Airport Consultants Council
- Airports Council International - North America
- American Association of Airport Executives
- The Boeing Company
- Cargo Airline Association
- National Air Carrier Association
- National Air Transportation Association
- National Business Aviation Association
- 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
- C.A.T. Eyes
- Con-Way, Inc.
- Detroit-Windsor Truck Ferry
- First Student, Inc.
- INDUS
- 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
- Schneider National
- Seaton & Husk, LP
- SLT Express
- Taxicab, Limousine & Paratransit Association
- Transportation Research Board of the National Academies
- Tri-State Motor Transit Company
- 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
- Metropolitan Transportation Authority
- New Jersey Transit Authority
- The Port Authority Trans-Hudson Corporation
- Rock Island County Metropolitan Mass Transit District
- San Francisco Municipal Transportation Agency
- Utah Transit Authority
- Washington Metropolitan Area Transit Authority

PIPELINE MODE SCC MEMBERS

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

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 155,000 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 and casualties, as well as interruptions in service that would impact public health and economic vitality. Protecting Water Sector infrastructure requires partnerships among Federal, State, local, tribal, and territorial governments and private sector infrastructure owners and operators, associations, and key stakeholders. These entities collaborate and coordinate effectively in order to assist drinking water and wastewater utilities increase resilience and prepare to prevent, detect, respond to, and recover from all hazards.

The Water Sector Coordinating Council (SCC) consists of 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 and 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.

VISION

A secure and resilient drinking water and wastewater infrastructure that provides clean and safe water as 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, outlined in the Water Sector-Specific Plan, 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:

- Granted the Support Anti-Terrorism by Fostering Effective Technologies Act designation by the U.S. Department of Homeland Security (DHS) for meeting the technical criteria through the development of two security practices standards:
  - *American National Standards Institute (ANSI)/American Water Works Association (AWWA) G430-09: Security Practices for Operations and Management*
  - *ANSI/American Society of Mechanical Engineers-Innovative Technologies Institute /AWWA J100-10: Risk Analysis and Management for Critical Asset Protection® -Standard for Risk and Resilience Management of Water and Wastewater Systems*
- Issued *ANSI/AWWA G440-11: Emergency Preparedness Practices*.
- Established a partnership agreement between the Water Information Sharing and Analysis Center (WaterISAC) and the National Cybersecurity and Communication Integration Center, and is leading the Water Sector's cybersecurity efforts as the sector's senior representative on the DHS Cyber Unified Coordination Group.
- Completed the deployment of, commenced analysis of, and began developing a publication of results from EPA's five Water Security Initiative pilots.
- Conducted full-scale exercises in conjunction with 25 Federal, State, local, and commercial laboratories.
- Supported the WaterISAC's mission to provide infrastructure protection information and tools to the Water Sector, thereby improving utility security and resilience from all hazards. Information and tools included threat alerts, briefings, and analyses on physical security and cybersecurity; a full-time water security analyst; Webinars and training; contaminant databases; and emergency preparedness resources.
- Completed development of the Water Health and Economic Analysis Tool's drinking water and wastewater modules for hazardous gas and loss of operating assets scenarios.
- Established the 48th Water/Wastewater Agency Response Network (WARN) and continued efforts to support its operational plans, outreach, and communications.
- Conducted nine water-specific training courses on how to use the Incident Command System and the National Incident Management System effectively during emergency response situations.
- Partnered with the Federal Bureau of Investigation, U.S. Food and Drug Administration, and the U.S. Department of Agriculture to sponsor three Multisector Infrastructure Protection and Threat Workshops.
- Completed integration of the National Environmental Methods Index for Chemical, Biological, and Radiological Methods data into the Water Contaminant Information Tool.
- Developed *Planning for an Emergency Water Supply* in response to provisions of the 2002 Bioterrorism Act through the collaborative efforts of EPA's National Homeland Security Research Center and AWWA.
- Developed the *Emergency Water Supply Planning for Hospitals and Healthcare Facilities* and the *Drinking Water Advisory Communication Toolbox* through the collaboration of the Centers for Disease Control and Prevention and AWWA.
- Released *Business Continuity Planning for Water Utilities* through collaborative efforts of the Water Research Foundation, AWWA, and EPA.

KEY INITIATIVES

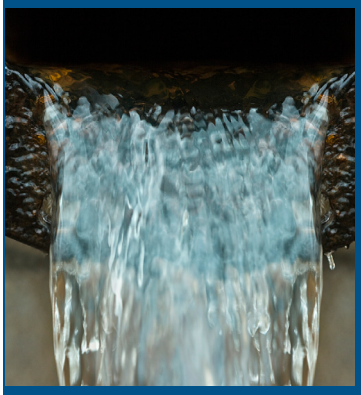
The Water Sector continues to focus its efforts on working collaboratively to minimize the obstacles owners and operators may face while trying to implement protective programs. Key initiatives within the sector include the following:

- Conducting pilots for drinking water contamination warning systems in five major U.S. cities and disseminating results to utilities across the country.
- Improving physical security, cybersecurity, and resilience with threat analyses and other infrastructure protection information and tools through the WaterISAC.
- Developing and promoting a broad range of water security, preparedness, and resilience efforts through training, emergency planning, security enhancements, journal articles, and conference presentations, as well as by leveraging the WaterISAC.
- Developing tools to help utilities enhance emergency response, preparedness, and resilience during and following incidents.
- Developing a laboratory network capable of providing analytical support and the capacity necessary to process an influx of samples during an emergency.

PATH FORWARD

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

- Continue research and development efforts through strategic planning as well as cybersecurity and decontamination development efforts.
- Advance the use, development, and exercising of WARN in response and business continuity planning.
- Continue working on the WaterISAC's mission and goals for increasing utility physical security and cybersecurity with threat analyses and other infrastructure protection information and tools.
- Enhance ongoing partnership efforts of the Water SCC, GCC, and Critical Infrastructure Partnership Advisory Council working groups.



GCC MEMBERS

- Association of State Drinking Water Administrators
- Association of State and Interstate Water Pollution Control Administrators
- Association of State and Territorial Health Officials
- Environmental Council of the States
- National Association of County and City Health Officials
- New York City, Department of Environmental Protection
- 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
- Boston Water and Sewer Commission
- Breezy Hill Water and Sewer Company
- California Water Service Company
- City of Portland Bureau of Environmental Services
- Gadsden Water Works and Sewer Board
- 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
- Northeast Ohio Regional Sewer District
- Onondaga County Water Authority
- Prince William County Service Authority
- Spartanburg Water
- Trinity River Authority of Texas
- United Water
- Water Environment Federation
- Water Environment Research Foundation
- Water Information Sharing and Analysis Center
- Water Research Foundation

Homeland Security