



Critical Infrastructure Partnership Advisory Council

Annual
2013



Homeland Security

Page intentionally left blank

CRITICAL INFRASTRUCTURE PARTNERSHIP ADVISORY COUNCIL

2013 ANNUAL

CONTENTS

CRITICAL INFRASTRUCTURE PARTNERSHIPS	1
CROSS-SECTOR PARTNERSHIPS	5
Critical Infrastructure Cross-Sector Council	5
Federal Senior Leadership Council	6
Regional Consortium Coordinating Council	7
State, Local, Tribal, and Territorial Government Coordinating Council	9
SECTOR PARTNERSHIPS	11
Chemical Sector	11
Commercial Facilities Sector	13
Communications Sector	15
Critical Manufacturing Sector	17
Dams Sector	19
Defense Industrial Base Sector	21
Emergency Services Sector	22
Energy Sector	24
Financial Services Sector	26
Food and Agriculture Sector	27
Government Facilities Sector	28
Healthcare and Public Health Sector	29
Information Technology Sector	31
Nuclear Reactors, Materials, and Waste Sector	33
Transportation Systems Sector	35
Water Sector	37

CRITICAL INFRASTRUCTURE PARTNERSHIPS

INTRODUCTION

The responsibilities of protecting the Nation’s diverse and complex critical infrastructure remain at the forefront of the U.S. Department of Homeland Security (DHS). As affirmed in February 2013, Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21) states: “proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure—including assets, networks, and systems—that are vital to public confidence and the Nation’s safety, prosperity, and well-being.”

Prior to the September 11, 2001 attacks on our Nation, three administrations and a number of national bipartisan commissions and councils—including the 1996 President’s Commission on Critical Infrastructure Protection—identified the protection of critical infrastructure as a national goal and recommended greater cooperation and communication through public-private partnerships as a means to reduce risks and vulnerabilities and to build resilience in the event of a terrorist act or natural disaster. Building on these recommendations and in response to public law, DHS issued the *National Infrastructure Protection Plan* (NIPP) in 2006, updated in 2009, and currently under revision as part of implementation of PPD-21. The NIPP provided a unifying framework to integrate a range of efforts designed to enhance the protection of the Nation’s critical infrastructure. The Critical Infrastructure Partnership Advisory Council (CIPAC) and national critical infrastructure partnership structures enable the collaboration and trusted information sharing necessary to accomplish these efforts.

This 2013 *Critical Infrastructure Partnership Advisory Council Annual* includes a description of CIPAC’s function and contributions, as well as a summary of the 2013 initiatives and the accomplishments of four cross-sector partnership councils and 16 critical infrastructure sector partnerships.¹

¹ The number of critical infrastructure sectors has changed over time, pursuant to Federal guidance. In guiding the NIPP, Homeland Security Policy Directive 7: Critical Infrastructure Identification, Prioritization, and Protection recognized 17 sectors, with Critical Manufacturing added as the 18th sector in 2008. PPD-21: Critical Infrastructure Security and Resilience, the most recent policy, identifies 16 sectors. This Annual is therefore organized by 16 sectors, with National Monuments and Icons Sector accomplishments included in the Government Facilities Sector chapter and Postal and Shipping Sector accomplishments included in the Transportation Systems Sector chapter.

THE NATIONAL CRITICAL INFRASTRUCTURE PARTNERSHIP STRUCTURE

Efforts to protect the Nation’s critical infrastructure have incorporated a wide variety of organizational structures, operating models, governance constructs, and systems that include distributed networks, interdependent physical functions and cyberfunctions. The national critical infrastructure partnership structures—including Sector Coordinating Councils (SCC), Government Coordinating Councils (GCC), and cross-sector partnership councils—facilitate this close cooperation and foster the trusted relationships necessary to manage critical infrastructure security and resilience in this inherently complex environment. Although many activities are planned and implemented within each sector’s respective partnership council, national partnership structures regularly convene private-sector and government partners under the auspices of CIPAC to jointly plan and implement critical infrastructure programs; to coordinate activities through joint strategies and roadmaps; and to contribute to national policies, plans, and programs.

Overall, as described throughout this Annual, GCCs and SCCs operating under the auspices of CIPAC have made advancements in information sharing, training and exercises, research and development, program evaluation, strategic planning, risk management, and sector-specific metrics development. For additional information on the national partnership structures please visit <http://www.dhs.gov/critical-infrastructure-sector-partnerships>.

CIPAC FUNCTION AND CONTRIBUTION

Recognizing that private-sector participation in the critical infrastructure mission is essential to strategic planning and effective information sharing, the DHS Secretary established CIPAC as an advisory council exempt from the Federal Advisory Committee Act under which private-sector partners may voluntarily collaborate with Federal Government agencies on critical infrastructure security and resilience efforts. As the principal means of implementing the critical infrastructure public-private partnership, CIPAC promotes coordinating, communicating, and sharing effective practices across critical infrastructure sectors, jurisdictions, or specifically defined geographical areas. These objectives are achieved

through a level of openness appropriate to support the homeland security mission, while maintaining a level of information surety needed for the private sector to be willing to share often sensitive critical infrastructure information.

The use of CIPAC to enable these foundational cross-government and public-private partnerships has increased over time and has evolved to address emerging issues, as highlighted by the following achievements:

- CIPAC member institutions increased from 962 in 2012 to 1,130 in 2013.
- In 2012, 60 working groups held meetings under CIPAC with 199 total meetings. In the first half of 2013, 42 working groups held meetings under CIPAC with 100 total meetings. The meetings' objectives included information sharing, training and exercises, research and development, program evaluation, strategic planning, risk management, and sector-specific metrics development.
- For the third year in a row, the Regional Partnership Engagement effort convened critical infrastructure owner and operator focus groups under CIPAC. More than 300 participants, representing 257 owners and operators from nearly all of the critical infrastructure sectors, detailed steps that DHS can take to better meet owner/operator security and resilience objectives and to strengthen the value of the public-private partnership. Approximately 50 recommendations from these CIPAC forums are currently being tracked for implementation.

For additional information on CIPAC, including membership and meeting information, please visit <http://www.dhs.gov/cipac>.

KEY INITIATIVES AND ACTIVITIES

The DHS National Protection and Programs Directorate's Office of Infrastructure Protection (IP) utilizes CIPAC forums to engage with public and private-sector critical infrastructure partners to understand the requirements and to implement security and resilience programs and policies reflecting stakeholder views. Over the past year, two primary initiatives—the Integrated Task Force (ITF) implementing Executive Order 13636: Improving Critical Infrastructure (EO 13636) and PPD-21 and the Regional Partnership Engagement—have utilized CIPAC to meet these goals.

Cybersecurity Executive Order and Critical Infrastructure Security & Resilience Presidential Policy Directive Integrated Task Force

In 2013, DHS began the process of implementing EO 13636 and PPD-21, the goal of which is to drive action toward system and network security and resilience and to enhance the efficiency and effectiveness of the U.S. Government's work to secure critical infrastructure and to improve its resilience. To accomplish this, DHS established the ITF to coordinate interagency, public, and private-sector efforts and to ensure the effective synchronization of activities across the homeland security enterprise.

Section 6 of EO 13636 directs the Secretary of Homeland Security to establish a "consultative process" to coordinate improvements to the cybersecurity of critical infrastructure. Specifically, EO 13636 states: "the Secretary shall engage and consider the advice, on matters set forth in this order, of the Critical Infrastructure Partnership Advisory Council; Sector Coordinating Councils; critical infrastructure owners and operators; Sector-Specific Agencies (SSAs); independent regulatory agencies; other relevant agencies; State, local, territorial, and tribal (SLTT) governments; universities; and outside experts."

Further, PPD-21 mandates a "national unity of effort" that includes "...expertise and day-to-day engagement from the SSAs as well as the specialized or support capabilities from other Federal departments and agencies, and strong collaboration with critical infrastructure owners and operators and SLTT entities."

To implement EO 13636 and PPD-21, the Executive Branch was directed to consult with critical infrastructure partners to understand the cascading consequences of infrastructure failures, evaluate the public-private partnership, promote cybersecurity practices, increase information sharing, and develop updated frameworks and plans for both physical security and cybersecurity.

With an average of two to three meetings per week, CIPAC, SCC, GCC, and cross-sector engagements proved critical to implementing the EO 13636 and PPD-21 directive to consult with critical infrastructure partners to understand the cascading consequences of infrastructure failures, evaluate the public-private partnership, and increase information sharing. Critical infrastructure partners were engaged in in-depth discussions through workgroups, focus groups, Webinars, roundtables, and meetings. Their contributions aided the completion of EO-PPD deliverables, including an updated national plan on critical infrastructure; a voluntary Cybersecurity Framework; a demonstration of a real-time information-sharing capability; and the identification of critical infrastructure that would reasonably affect

our national security, economic security, public health, and safety if affected by a cybersecurity incident.

NPPD and IP will build upon this consultative process by convening CIPAC forums throughout the Nation to support proactive steps undertaken jointly by government and private-sector partners to manage risks and strengthen national critical infrastructure security and resilience.

For additional information on the ITF and implementation of EO 13636 and PPD-21, please visit: <http://dhs.gov/strengthening-security-and-resilience-nation's-critical-infrastructure>.

Executive Order on Improving Chemical Facility Safety and Security

On August 1, 2013 the President signed Executive Order 13650 to improve the safety and security of chemical facilities and reduce the risks of hazardous chemicals to workers and communities.

The Executive Order on Improving Chemical Facility Safety and Security directs the Federal Government to:

- improve operational coordination with State and local partners;
- enhance Federal agency coordination and information sharing;
- modernize policies, regulations, and standards; and
- work with stakeholders to identify best practices.

These measures and continued collaboration with state, local, tribal, industry, and community partners will help to significantly improve the safety and security of chemical facilities throughout the nation while minimizing any additional burden on owners and operators.

For more information on the Chemical Executive Order Working Group, go to <http://www.dhs.gov/chemical-security> or email eo.chemical@hq.dhs.gov.

Regional Partnership Engagement

In 2011, IP has transitioned its Regional Initiative to the on-going Regional Partnership Engagement effort to engage public- and private-sector partners at a regional level to better understand the critical infrastructure security and resilience requirements. Partner feedback assists IP in developing programs that more accurately inform risk-management investments and actions in the field. To date, CIPAC provided a forum for 14 critical infrastructure owner and operator focus groups to convene in seven Federal regions. In addition to providing valuable input to IP, these focus groups provide owners and

operators an opportunity to build connections with peers and to exchange ideas and approaches related to security and business continuity. Sample findings and recommendations generated by the focus groups include:

- Perimeter monitoring, access control, and exercises and training are priority security investments that promote employee readiness and awareness.
- Facility assessments compare security practices against sector peers, identify security gaps based on outside validation, and gain buy-in for security investments.
- Partnerships facilitate an understanding of capabilities and responsibilities, the sharing of best practices and information, and working together during emergencies.
- Prevalent recommendations included: sponsor venues to facilitate partnership development; the development of new training and exercise topics; market critical infrastructure programs and training opportunities; and enhancing the understanding of synergies, dependencies, and interdependencies.

The Regional Partnership Engagement also draws input from State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) Regional Reports and Joint Critical Infrastructure Partnership (JCIP) Workshops. The Regional Reports, which study critical infrastructure programs in all 10 Federal regions, help SLTT critical infrastructure personnel learn about and benefit from the approaches used by colleagues in different regions. The 2013 JCIP Workshops, a joint effort between IP and the Regional Consortium Coordinating Council, serve as the Regional Partnership Engagement component with the broadest outreach to critical infrastructure partners. Cross-sector Webinar discussions focus on how best to integrate private-sector partners into DHS programs and educating participants on resources available to them. Reports produced under this effort are accessible to partners via the Homeland Security Information Network—Critical Infrastructure (HSIN-CI).

Following these successful partnership engagements and documentation of partner needs and requirements, the Regional Partnership Engagement is entering into a new phase focused on the resulting outcomes. IP is leading the effort to actively review and track the progress of all partner recommendations received through the effort. Primary steps include collaborating with the appropriate division or agency to adjudicate each recommendation and engaging the Sector Partnership networks, including the cross-sector councils to review the recommendations' status.

This collaboration will also support partners' critical infrastructure efforts and will foster regional interdependencies and resilience.

2014 SECTOR AND CROSS-SECTOR PRIORITIES

CIPAC provides an opportunity for Government and owners and operators to work together to advance the Nation's critical infrastructure security and resilience. Sustaining 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 2014:

- Support efforts to implement PPD-21 and EO 13636 at the sector level
 - Continue to engage owners and operators on the importance of integrating physical security and cybersecurity into preparedness efforts
 - Integrate PPD-21 and EO 13636 into 2014 planning efforts
 - Develop revised goals, objectives, and associated implementation actions that incorporate elements of PPD-21 and EO 13636 into Sector-Specific Plans
- Maintain and promote a collaborative environment for sector partners to improve risk-management and information-sharing activities
 - Coordinate seminars or workshops to provide owners and operators with opportunities to test their information-sharing mechanisms
 - Pursue a partnership-oriented approach to refine, develop, and implement strategies and program implementation plans vital to the protection and resilience of the sectors
 - Pursue the active engagement of SCC counterparts and all sector partners to refine existing processes and to develop new processes required to eliminate unacceptable levels of risk
 - Leverage existing channels of communication and build additional channels through State and local partnerships

- Expand stakeholder knowledge and understanding of Federal critical infrastructure resources, tools, and capabilities
 - Maximize outreach efforts to owners and operators, industry stakeholders, and first-responder communities to introduce them to federally sponsored programs
 - 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 activities and initiatives on specific areas of concern and attention, including interdependencies, cybersecurity, and critical asset identification
 - Determine criteria for developing an effective program to characterize and identify critical infrastructure assets
 - Improve awareness of interdependencies among sectors and agencies to 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
- Continue with efforts to develop physical, cybersecurity, reliability, and resilience metrics that can be used to track and report on activities and advances



CRITICAL INFRASTRUCTURE CROSS-SECTOR COUNCIL

Cross-sector issues and interdependencies are addressed among the Sector Coordinating Councils (SCCs) through the Critical Infrastructure Cross-Sector Council. The Partnership for Critical Infrastructure Security (PCIS) provides this representation by convening leadership and member companies and organizations of each SCC as the industry companion to the Federal Senior Leadership Council (FSLC).

The PCIS was chartered in 1999 and remains active in the mission to work collaboratively with government partners and community stakeholders to improve the security and resilience of our Nation's critical infrastructure. Council activities include providing senior-level, cross-sector strategic coordination within private sector critical infrastructure and through partnerships with the U.S. Department of Homeland Security (DHS) and 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 actions and best practices to identify, assess, and manage risk to improve cybersecurity and critical infrastructure security and resilience, preparedness, and resilience across sectors and the critical infrastructure community.

SELECTED ACCOMPLISHMENTS

The Council's recent accomplishments include the following:

- Enhanced collaboration between PCIS, the State, Local, Tribal and Territorial Government Coordinating Council, Regional Consortium Coordinating Council, National Council of Information Sharing and Analysis Centers (ISACs), and other stakeholders
- Coordinated efforts with industry and government partners through the Cross-Sector Cybersecurity Working Group to improve and enhance the U.S. national cybersecurity profile
- Developed a strategic proposal and operational approach to achieving effective, predictable, and sustainable sharing of threat intelligence working with and through the Joint Threat Intelligence & Security Engagement Working Group
- Participated in joint meetings with the FSLC
- Participated in the National Level Exercise Program
- Conducted a workshop with the ISACs to highlight accomplishments of various critical infrastructure sectors and upcoming initiatives
- Provided the Integrated Task Force with regular feedback on the implementation of Presidential Policy Directive 21: Critical Infrastructure Security and Resilience and Executive Order 13636: Improving Critical Infrastructure through participation in various working groups
- Developed the *Proposed Strategy for Enhancing the Public-Private Partnership* to sustain conditions that enable the effective application of the spectrum of capabilities, expertise, and experience for the security and resilience of the Nation's critical infrastructure
- Worked with DHS, the Federal Bureau of Investigation, and the National Security Agency to develop a Webinar series to raise awareness and educate chief information officers, chief security officers, and other stakeholders responsible for cybersecurity and critical infrastructure protection risk management by drawing on lessons learned from previous cyberevents that were successful, unsuccessful, interrupted, or disrupted. The focus is on information and analysis related to tactics, techniques, and procedures pursued by perpetrators and how that experience may inform protective measures and risk-management decisionmaking for a broad range of stakeholders.

FEDERAL SENIOR LEADERSHIP COUNCIL

The Federal Senior Leadership Council (FSLC) enhances communication, collaboration, and coordination among senior executives of Federal departments and agencies with a role in implementing the *National Infrastructure Protection Plan* (NIPP) and facilitates critical infrastructure security and resilience efforts nationwide and internationally. FSLC members include the Sector-Specific Agency (SSA) for each critical infrastructure sector, as well as several additional agencies with responsibilities in critical infrastructure security and resilience. 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).

SELECTED ACCOMPLISHMENTS

Recent accomplishments of FSLC agencies include the following:

- Collaborated with interagency, public, and private partners to implement deliverables required by Executive Order 13636: Improving Critical Infrastructure (EO 13636) and Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21), while maintaining effective integration and implementation across the homeland security enterprise
- Participated in Integrated Task Force working groups to drive action toward system and network security and resilience, as well as to enhance the efficiency and effectiveness of the government's work to secure critical infrastructure as directed by EO 13636 and PPD-21
- Conducted joint meetings in December 2012 and July 2013 with leadership of the SLTTGCC, Partnership for Critical Infrastructure Security,

Regional Consortium Coordinating Council, and National Council of Information Sharing and Analysis Centers to review initiatives and issues of common interest among critical infrastructure partners

- Participated throughout the year in cross-sector teleconferences and Webinars with the U.S. Department of Homeland Security; State, local, tribal, and territorial governments; and private-sector critical infrastructure partners to discuss new and evolving threats to critical infrastructure security

KEY INITIATIVES

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 security 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 security 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 security and resilience activities in the Sector Annual Reports and the *Critical Infrastructure Partnership Advisory Council Annual*

REGIONAL CONSORTIUM COORDINATING COUNCIL

Regional critical infrastructure partnerships involve multijurisdictional, cross-sector, and public-private sector efforts focused on the preparedness, security, response, and resilience 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 (RC3) in July 2008 as a self-organized, self-governed body focused on addressing regional challenges in implementing the NIPP.

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 RC3 identified the following goals:

- Promoting and fostering protection and resilience efforts
- Developing a national policy framework for regional infrastructure protection, prevention, deterrence, response, recovery, and longer-term restoration
- Providing the foundation for regional cross-sector collaboration
- Fostering the development of risk-based protection and mitigation measures to enable measurable progress toward robust security and disaster resilience
- Enhancing the education and awareness of critical infrastructure interdependencies

SELECTED ACCOMPLISHMENTS

Recent RC3 accomplishments include the following:

- Increased membership and regional representation by approving the Great Lakes Hazards Coalition as a member of the RC3 Executive Committee
- Maintained an interactive, dynamic Website

- Established a social media presence that includes Facebook, Twitter, and YouTube
- Hosted the 2013 Annual RC3 Full Member Plenary to coincide with the 2013 National Homeland Security Conference and enabled members to attend both sessions
- Participated in the DHS National Protection and Programs Directorate's Office of Infrastructure Protection (IP) Evaluation and Planning Working Group and participated in the DHS Integrated Task Force to share recommendations for improving the partnership model
- Coordinated with DHS IP to develop an active shooter presentation and materials for RC3 members

KEY INITIATIVES

The RC3 is engaged in various initiatives to advance critical infrastructure security, vulnerability reduction, and consequence mitigation, including the following:

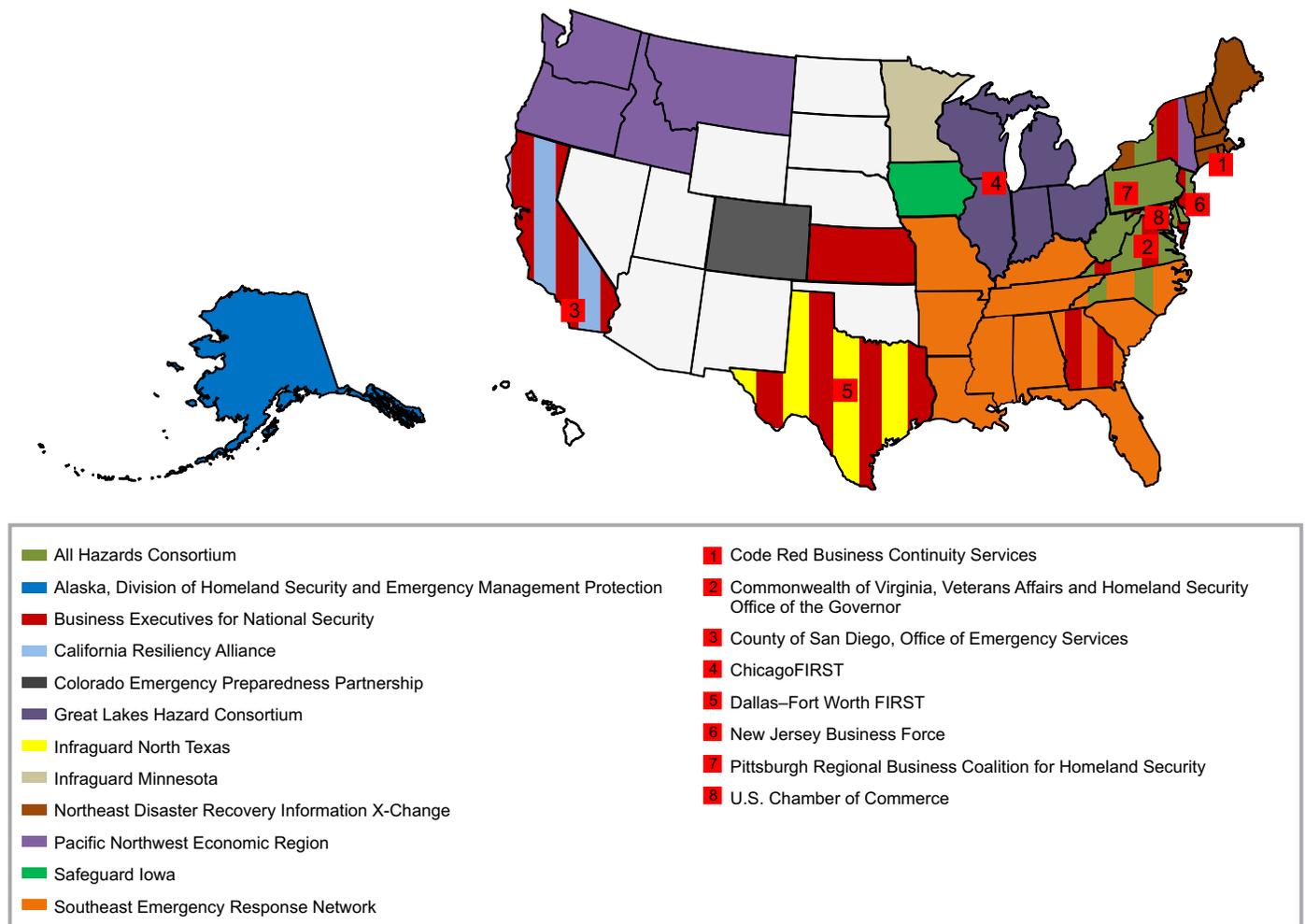
- Enhancing education and awareness of critical infrastructure interdependencies
- Partnering with the Critical Infrastructure Cross-Sector Council and the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) to improve information sharing and communication throughout the NIPP Sector Partnership and leverage each other's membership and knowledge
- Hosting Webinars to enhance partners' understanding of the roles of the RC3, Critical Infrastructure Cross-Sector Council, and SLTTGCC in critical infrastructure security and resilience
- Conducting regional catastrophic event response and recovery exercises in conjunction with existing regional workshops
- Identifying best practices and standards for using social media tools in critical infrastructure security and resilience
- Developing a communication and collaboration strategy that embraces social media 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 RC3 developed an aggressive plan to accelerate its maturation through 2013 and beyond. Steps to move the RC3 forward in achieving its goals include the following:

- Establish working groups to foster collaboration and build consensus across regional partnerships
 - Reach out to the critical infrastructure community to develop strong partnerships with leaders that demonstrate prolific protection and resilience efforts
 - Identify additional regional partnership engagement activities to sponsor and/or engage RC3 members and partners
- Advance supporting partnerships, collaborations, and tools that will provide the greatest force-multiplying effect across regional partnerships, such as Geographic Information Systems and social media efforts that increase situational awareness in planning and responding to events threatening U.S. critical infrastructure
 - Continue building structures that will enable the RC3 to assist with national-level policy discussions that affect regional critical infrastructure entities, owners, and operators

REGIONAL CONSORTIUM COORDINATING COUNCIL MAP OF PARTICIPANTS



For a complete list of RC3 members, please visit <http://rtriplec.wordpress.com/members/>.

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 process of planning, implementing, and evaluating the national critical infrastructure security and resilience mission. The SLTTGCC includes representatives from SLTT governments and provides a view into the diverse perspectives, priorities, and needs of governments across the Nation, as well as a central hub for State, local, and regional officials to coordinate on critical infrastructure security and resilience challenges.

The SLTTGCC currently has 36 members—including homeland security advisors, law enforcement officials, critical infrastructure coordinators, public health officials, emergency managers, fire services representatives, and information security officials—from State, county, municipality, tribal, and territorial governments. In addition, the SLTTGCC integrates multidisciplinary perspectives through its involvement in the NIPP Sector Partnership and engages numerous subject matter experts to broaden and inform its perspectives. The SLTTGCC adds representation from additional organizations—such as transportation departments or port authorities—when possible. SLTTGCC members also serve as liaisons to sector Government Coordinating Councils (GCCs), representing SLTT perspectives at GCC and joint GCC-Sector Coordinating Council meetings.

VISION

The SLTTGCC vision is to foster dialogue among all levels of government to fulfill the critical infrastructure security 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 security and resilience efforts.
- Encourage the integration of SLTT government perspectives into Federal planning efforts and promote regional coordination with 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 via the Homeland Security Information Network-Critical Infrastructure platform (HSIN-CI)
- Engage with and leverage academic resources and the national laboratory system in furthering SLTTGCC work on behalf of SLTT governments

SELECTED ACCOMPLISHMENTS

SLTTGCC accomplishments over the past year include the following:

- In conjunction with the 2012 Critical Infrastructure Partnership Advisory Council Plenary, held a successful plenary session in October 2012 focused on improving resilience against natural disasters
- Produced five regional landscape study reports examining State and local critical infrastructure security and resilience programs in five different Federal regions of the country. The reports serve as a baseline to identify best practices and innovative approaches to bolster critical infrastructure and security resilience efforts in other SLTT jurisdictions.

- Authored *Landscape Report: State Entities Participating in a Public-Private Partnership Environment*, which describes State open records and open meetings laws and how they affect information sharing with critical infrastructure owners and operators
 - Authored *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
 - Authored *White Paper—Tribal Critical Infrastructure Priorities and Needs*, which examines critical infrastructure security and resilience on tribal lands, including the applicability of DHS Office of Infrastructure Protection (IP) programs to tribes and best practices for collaboration between IP and tribal nations
 - Established a temporary working group to provide feedback to the DHS Office of Health Affairs regarding the prioritization of the anthrax vaccine to the critical infrastructure sectors. This feedback was utilized in producing the *Guidance for Protecting Responders' Health During the First Week Following a Wide-Area Aerosol Anthrax Attack*.
 - Provided the DHS Integrated Task Force with regular feedback on the implementation of Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21) and Executive Order 13636: Improving Critical Infrastructure (EO 13636) through Webinars and participation in various working groups
- Developing a series of baseline reports to help critical infrastructure security and resilience staff share the approaches and practices that their colleagues in different regions have taken to advance infrastructure security and resilience. To date, the SLTTGCC has produced reports that include nine Federal regions and will complete a baseline report for the remaining region in 2013.
- Supporting the critical infrastructure owner and operator focus groups and the Joint Critical Infrastructure Partnership Workshops with DHS
 - Institutionalizing the Critical Infrastructure Protection Coordinator Alliance Network in partnership with DHS. The 165-member network enables SLTT mission partners to network, share best practices, and provide DHS and the SSAs with regular feedback on requirements and programs.
 - Providing members of the Alliance Network with access to its CI Council portal and materials
 - Sponsoring the monthly Real-Time Forum series (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 baseline study of State and local critical infrastructure security and resilience programs in each Federal region
- Continue to grow the Critical Infrastructure Protection Coordinator Alliance Network and sustain the monthly Real-Time Forum series
- Provide DHS with regular feedback on its programs and tools, including recommendations associated with the DHS transition to a single assessment methodology
- Strengthen its Sector Liaison program to ensure effective SLTT representation on the GCCs
- Continue to evaluate HSIN-CI as a communication vehicle and recommend improvements
- Contribute to the implementation of PPD-21 and EO 13636
- Broaden and diversify its pool of members and subject matter experts

For a complete list of SLTTGCC members, please visit <http://www.dhs.gov/current-slttgcc-members>.

KEY INITIATIVES

The SLTTGCC conducts most of its activities through working groups. For a complete list of these working groups, please visit <http://www.dhs.gov/working-groups-state-local-tribal-and-territorial-government-coordinating-council>.

The SLTTGCC continues to support initiatives designed to extend the value of its activities to SLTT critical infrastructure security and resilience programs across the Nation, including IP's Regional Partnership Engagement and Critical Infrastructure Protection Coordinator Alliance Network.

Contributions include the following:

- Studying the SLTT critical infrastructure security and resilience programs in each of the 10 Federal regions



Chemical Sector

The Chemical Sector—with 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 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. The industry implements a variety of voluntary security programs and continues to make significant capital investments to address security concerns. For more information on the sector's vision, goals, and risk-management approach, please see the [Chemical Sector Snapshot](#) and the 2010 [Chemical Sector-Specific Plan](#).

SELECTED ACCOMPLISHMENTS

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

- Continued implementation of Chemical Facility Anti-Terrorism Standards (CFATS) for the highest-risk facilities in the sector. As of June 24, 2013, 3,375 facilities have been assigned a final tier and 930 are awaiting a final tier assignment. Since the program's inception, 493 plans have been authorized, 339 authorization inspections have been conducted, and 134 plans have been approved.
- Coordinated the seventh annual Chemical Sector Security Summit in July 2013
- Certified more than 14,700 individuals who have completed the Web-based Chemical Security Awareness Training Program since its launch in July 2008
- 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
- Continued to acquire new users of the Voluntary Chemical Assessment Tool. The 544 users have completed 210 facility assessments as of June 22, and 77 are in progress.
- Promoted the Chemical Sector Preparedness Accreditation and Certification Program Framework Guides
- Worked with the Chemical Sector Coordinating Council (SCC) and the American Chemistry Council to develop Chemical Sector Emergency Response Standard Operating Procedures to ensure consistency during national incidents of significance. A tabletop exercise was completed utilizing the events of Superstorm Sandy, which gave SCC members and partners an opportunity to discuss roles, responsibilities, and interactions between government and Chemical Sector critical infrastructure partners.
- Participated actively in listening sessions for Executive Order 13636: Improving Critical Infrastructure (EO 13636) and Presidential Policy Directive-21: Critical Infrastructure Security and Resilience (PPD-21), to provide recommendations on implementation options being considered by the Integrated Task Force led by the U.S. Department of Homeland Security (DHS)
- Formed a joint cybersecurity working group of representatives of the Chemical, Oil and Natural Gas, and Pipeline Sector Coordinating Councils to consider the many mutual cybersecurity concerns across the three sectors and coordinate on recommendations on implementation of EO 13636

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 through collaboration with DHS and industry partners
- Enhancing information sharing through the Chemical Sector Security Summit, Classified Chemical Sector Briefings, monthly threat teleconferences held jointly with the Oil and Natural Gas Subsector, the Chemical Sector Training and Resources Website, and the Homeland Security Information Network – Critical Infrastructure
- Developing and promoting free Web-based tools, training, and best practices documents for easy access by all sector partners

- Providing training opportunities to improve preparedness and response through the Ammonia Safety and Training Institute and Transportation Community Awareness and Emergency Response efforts
- Continuing to implement the *Roadmap to Secure Control Systems in the Chemical Sector* that includes completion and distribution of *Making the Business Case*, a document which encourages companies to improve overall security
- Rolling out recently developed theft and diversion training to sector members to ensure awareness of the issue
- Encourage an ongoing public-private dialogue through the National Infrastructure Protection Plan 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

PATH FORWARD

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

- Continue development of the Incident Communication Standard Operating Procedures for incident reporting and awareness among Chemical SCC members and their partners
- Work with Congress and other security partners to obtain permanent congressional authorization for CFATS
- Continue to enhance established Chemical Sector partnerships by improving communications between private-sector and Federal partners, and resolving scheduling conflicts with planning private-sector meetings
- Maximize outreach efforts to owners and operators, State chemical industry councils, and first-responder communities to introduce them to free programs sponsored by the Sector-Specific Agency
- Continue to engage Chemical Sector owners and operators on the importance of integrating physical security and cybersecurity
- Implement the Personnel Surety Program, a key component of facility security, under which CFATS-regulated facilities will submit personnel information for vetting against the Terrorist Screening Database
- Foster the security of ammonium nitrate by moving forward with the proposed Ammonium Nitrate Security Program rulemaking process



Commercial Facilities Sector

The Commercial Facilities Sector has a dominant influence on the Nation's economy. Facilities within the sector (e.g., stadiums, entertainment districts, theme parks, retail centers) operate on the principle of open public access, meaning that the general public can move freely throughout these facilities without the deterrent of highly visible security barriers. As the majority of these facilities are privately owned and operated, asset protection cooperation with the Federal Government is a relatively new concept for the sector. For more information on the sector's vision, goals, and risk-management approach, please see the [Commercial Facilities Sector Snapshot](#) and the 2010 [Commercial Facilities Sector-Specific Plan](#).

SELECTED ACCOMPLISHMENTS

Private- and public-sector partners in the Commercial Facilities Sector have made numerous accomplishments in bolstering sector protection and resilience. Accomplishments over the past year include the following:

- Expanded cyberengagement throughout the sector through the expansion of the Cyber Working Group
- Developed a sixth Risk Self-Assessment Tool (RSAT) module specifically tailored to address risks to shopping centers
- Conducted briefings to partners with equities in the London 2012 Olympics
- Developed a pre-incident preparedness checklist for private-sector partners to help them gather information needed to enhance the common operating picture when National Level Reporting is initiated
- Hosted a "Hurricane Sandy: 6 Months Later" teleconference with sector partners to capture lessons learned in planning for, responding to, and recovering from the effects of Superstorm Sandy
- Developed the Cybersecurity in the Gaming Subsector Webinar in collaboration with the National Cybersecurity Division
- Developed the Gaming Information-Sharing Tabletop Exercise in collaboration with the Exercise and Readiness Division
- Conducted four Outdoor Events Subsector Information-Sharing Tabletop Exercises
- Developed a Protecting Critical Infrastructure against Insider Threats course through the Federal Emergency Management Agency Emergency Management Institute
- Re-energized the Public Assembly Subsector Council through the development of a formal charter and the establishment of quarterly meetings
- Conducted two unclassified threat briefs to the National Association of Theater Owners in the aftermath of the Aurora, CO theater shooting
- Created the *Sports Venue Credentialing Guide* and *Sports Venue Bag Search Procedures Guide* for U.S. sports leagues and public assembly venues
- Developed and conducted the Insider Threat Awareness Virtual Roundtable Webinar in conjunction with the Federal Bureau of Investigation and Carnegie Mellon's Insider Threat Laboratory
- Created the Conducting Security Assessments: A Guide for Schools and Houses of Worship Webinar to support the White House plan to reduce gun violence
- Helped develop and pilot the Integrated Rapid Visual Screening tool, which provides mechanisms to conduct risk assessments and provide risk management for Federal facilities
- Supported development of the *Occupant Emergency Programs: An Interagency Security Committee Guide* to inform department and agency security planners creating and reviewing occupant emergency programs for the safety and security of employees and visitors at nonmilitary Federal facilities
- Improved information sharing by adding approximately 400 new documents to the Commercial Facilities Homeland Security Information Network (HSIN) portal and increasing the number of HSIN-Critical Infrastructure, Commercial Facilities Portal members by over 50 percent from last year

KEY INITIATIVES

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

- Providing explicit risk-mitigation guidance to owners and operators through U.S. Department of Homeland Security 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 Sector-Specific Agency outreach program
- Fostering an educational framework in which risk methodologies can be explored and understood for training purposes through programs offered by the National Center for Spectator Sports Safety and Security and classes offered by the International Association of Assembly Managers' Academy for Venue Safety and Security
- Expanding the use of the RSAT for stadiums and arenas, performing arts centers, lodging, convention centers, racetracks, theme parks, and shopping centers
- Leveraging the Commercial Facilities Suspicious Activity Reporting (SAR) Tool, which allows 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 sector moves forward in protecting and enhancing the resilience of its critical infrastructure. These steps include the following:

- Engage the U.S. Department of State and Transportation Security Administration to discuss overseas travel best practices and hazardous weather planning; update the *Protective Measures Guide for Sports Leagues*; expand and strengthen council alliances; and create a secure portal for subsector documents, products, and trusted vendor lists.
- Engage and develop a Big Box Store Subsector and organize a meeting for the group
- Host the Gaming Information-Sharing Tabletop Exercise, a series of five exercises beginning in May 2013, with support from the Stakeholder Readiness and Exercise Section
- 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
- Improve the quality, quantity, and timeliness of actionable threat information to help facilities identify appropriate responses to potential threats
- Continue to highlight the importance of cybersecurity by engaging sector partners through numerous forums, such as the Cross-Sector Cybersecurity Working Group and *National Strategy for Trusted Identities in Cyberspace*



Communications Sector

The Communications Sector is an integral component of the U.S. economy and is critical to the operation of all businesses, public safety organizations, government services, and our national security. Communications Sector technologies include wireline, wireless, satellite, cable, and broadcasting transport networks that support Internet, voice, data, and other key services. As part of

the larger global telecommunications infrastructure, these technologies and their associated services are interconnected. This interdependency makes protecting sector assets, systems, and networks even more critical to domestic security. Through public-private partnerships, the sector has been able to increase the resilience of communications infrastructure in the face of emergencies and disasters. For more information on the sector's vision, goals, and risk-management approach, please see the [Communications Sector Snapshot](#) and the 2010 [Communications Sector-Specific Plan](#).

SELECTED ACCOMPLISHMENTS

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

- Participated in the New Jersey Office of Homeland Security and Preparedness Communications After-Action Workshop on Superstorm Sandy with State and local partners to evaluate pre-, during, and post-event common preparedness goals
- Collaborated with government and industry partners to develop a National Public Safety Broadband Network (NPSBN) Cyber Risk Assessment to assess the risks associated with the deployment of a dedicated Long Term Evolution public safety interoperable communications network for emergency responders
- Completed Phase I of the 2012 National Sector Risk Assessment (NSRA) for Communications, a joint public-private initiative that identified elevated physical risks, cyberrisks, and human risks to improve the security and resilience of the Nation's communications systems
- Updated the *National Emergency Communications Plan* with industry partners to leverage and incorporate private-sector and tribal input
- Completed the National Security Telecommunications Advisory Committee (NSTAC) *Report to the President on the National Security and Emergency Preparedness Implications of a Nationwide Public Safety Broadband Network*
- Coordinated bimonthly Network Security Information Exchanges (NSIE) meetings and the 2013 NSIE Multilateral Meeting, which convened NSIE, government, and private-sector representatives to discuss information sharing; advanced persistent threats; and best practices related to supply chain and workplace cybersecurity technology management
- Completed the NSTAC *Report to the President on Cloud Computing*
- Conducted joint exercises and training initiatives such as Eagle Horizon, one of four major exercises conducted during National Level Exercise 2012
- Worked with private-sector partners to improve cross-sector coordination mechanisms and address critical interdependencies through the Cross-Sector Cybersecurity Working Group

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:

- Participating in Communications Sector-related implementation activities described in Executive Order 13636: Improving Critical Infrastructure Cybersecurity (EO 13636), and Presidential Policy Directive-21: Critical Infrastructure Security and Resilience (PPD-21)
- Coordinating with the National Security/Emergency Preparedness (NS/EP) Communications Executive Committee Joint Program Office engagement with industry, examining all government NS/EP communications working groups and partnerships. Ensuring that these partnerships are effective and non-duplicative and that they validate specific mission needs.
- Reviewing Global Positioning System/Position, Navigation, and Timing Resilience with industry partners and examining the systems that support or enable critical functions for the sector
- Reviewing Out-of-Band Networks with private-sector partners to develop a design and associated cost estimates to address a separate out-of-band data network

- Updating the 2009 *National Emergency Communications Plan* with public and private-sector partners
- Completing Phase II of the 2012 NSRA to reduce elevated risks across the Communications Sector
- Working with industry to improve cross-sector coordination mechanisms and address critical interdependencies, including cybersecurity interdependencies
- Improving information-sharing programs for government and industry partners at the Federal, State, local, tribal, and territorial levels
- Conducting exercises and training initiatives with government and industry to enhance critical infrastructure security and response
- Mitigating network congestion or disruption via priority services programs such as Government Emergency Telecommunications Service, Wireless Priority Service, and Telecommunications Service Priority
- Coordinating bimonthly meetings and planning for the 2014 NSIE Multilateral Meeting
- Assisting international partners to further develop and improve NSIE to mitigate cyberintrusions in public telephone networks
- Facilitating supply chain risk management (SCRM) discussions between government and industry partners and collecting SCRM best practices through the Communications Sector Supply Chain Working Group

PATH FORWARD

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

- Continue to work with sector partners to develop risk-management solutions to inform public- and private-sector partners
- Continue to support the development of Next Generation Networks priority services to meet the evolving requirements of critical 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 NPSBN
- Improve outreach programs to further educate Communications Sector customers and other infrastructure owners and operators about communications infrastructure resilience and risk-management practices
- Promote educational programs and awareness of evolving communications technologies and their potential points of failure during emergencies
- Promote timely, relevant, and accurate sector threat information sharing between law enforcement, intelligence communities, and State and local decision makers with the appropriate industry partners



Critical Manufacturing Sector

The Critical Manufacturing Sector is crucial to the economic prosperity and continuity of the United States. The sector is composed of four broad manufacturing industries: primary metal manufacturing; machinery manufacturing; electrical and electronic equipment, appliance, and component manufacturing; and transportation equipment. Products designed and produced 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. Therefore, a direct attack on or disruption of elements of the manufacturing industry could disrupt essential functions at the national level and across multiple critical infrastructure sectors. For more information on the sector's vision, goals, and risk-management approach, please see the [Critical Manufacturing Sector Snapshot](#) and the 2010 [Critical Manufacturing Sector-Specific Plan](#).

SELECTED ACCOMPLISHMENTS

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

- Developed and distributed the Business Continuity Planning Suite, which creates tailored plans that meet individual company needs to increase the resilience of business to all hazards through analysis, development, and testing
- Expanded the membership of the Critical Manufacturing Sector Coordinating Council (SCC) as part of ongoing outreach efforts
- Created a more representative SCC by providing an outreach initiative tailored to regional small- and medium-sized manufacturers
- Held the Critical Manufacturing Sector Security Conference in Peoria, Illinois in September 2012, with attendance from the Critical Manufacturing SCC and Government Coordinating Council (GCC), and other private and public sector entities
- 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
- Continued two-way information sharing among SCC and GCC members through the Information Sharing Working Group (ISWG), 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. 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 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
- Hosted the second annual Partnership Road Show to inform partners of available government resources for enhancing their security and resilience. Created the pilot Critical Manufacturing Cross-Border Working Group, focusing on the northern border.
- Hosted the Annual Critical Manufacturing Security Conference, August 6–7, 2013, featuring presenters from the government and private sector speaking on topics requested by the SCC
- Hosted the Critical Manufacturing Cyber Road Show, June 18–19, 2013, featuring a series of security briefings and tours of select government facilities

KEY INITIATIVES

Sector partners are engaging in a wide variety of activities to mitigate risks to critical infrastructure, including the following:

- Identifying and reviewing the critical assets of each of the Critical Manufacturing Sector's functional areas
- Assessing and prioritizing risks to the sector's functional areas
- 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 that are essential to the sector’s effective recovery following an incident
- Measuring the effectiveness of the sector’s critical infrastructure security and resilience efforts
- Developing a means for reporting on critical infrastructure security and resilience effectiveness to relevant partners throughout Federal, State, and local governments, as well as the private sector
- Improving situational awareness during normal operations, developing situations, and actual incidents
- Developing threat indicators and warnings and sharing appropriate threat and vulnerability information with sector partners
- Participating in exercises to validate communication protocols, response plans, and procedures 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:

- Focus on the Cybersecurity Implementation and Response for the Critical Manufacturing SCC
- Continue actions of the Critical Manufacturing SCC ISWG, a key means of ensuring effective and meaningful information sharing among industry members as well as with the government
- Engage the Critical Manufacturing SCC Cybersecurity Working Group to better understand resources available from the government



Dams Sector

The Dams Sector includes dam projects, hydropower generation facilities, navigation locks, levees, dikes, hurricane barriers, industrial waste impoundments, mine tailings, and other water retention and water control facilities. It is a vital part of our Nation's infrastructure and provides a wide range of economic, environmental, and social benefits, including hydroelectric power, river navigation, water supply, wildlife habitat, waste management, flood control, and recreation. For more information on the sector's vision, goals, and risk-management approach, please see the [Dams Sector Snapshot](#) and the 2010 [Dams Sector-Specific Plan](#).

SELECTED ACCOMPLISHMENTS

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

- Continued development and implementation of enhancements to the *Dams Sector Analysis Tool (DSAT)*, which is a collaborative effort between the U.S. Department of Homeland Security (DHS) and the U.S. Army Corps of Engineers (USACE). DSAT is a powerful Web-based tool that provides secure access to a wide range of state-of-the-art analytical resources, including the automated flood simulation, inundation mapping, and consequence analysis capabilities developed through the National Center for Computational Hydroscience and Engineering at the University of Mississippi.
- Conducted multiple DSAT Webinars and specialty workshops to familiarize sector partners with its modules and applications. A successful training pilot effort was hosted by Federal Emergency Management Agency (FEMA) Region IV in May 2013, in collaboration with USACE, the Association of State Dam Safety Officials (ASDSO), and other DHS components. The goal of this training pilot, which included participants from FEMA Regions IV and VIII, was to familiarize emergency managers and State dam safety personnel with the automated flood inundation modeling capabilities available through DSAT in preparation for the 2013 Hurricane Season.
- Conducted the 2013 *Dams Sector Information Sharing Drill* in February 2013 to provide sector partners with an opportunity to test and validate information-sharing mechanisms and communication protocols under heightened physical- and cyber-threat conditions. The drill, which consisted of three days of virtual play representing a compressed timeframe, included more than 110 participants representing 37 different Federal, State, local, and private-sector organizations.
- Held the 2012 *Annual National Dam Security Forum* in conjunction with the 2012 Dam Safety Conference in September 2012. The forum, organized in collaboration with ASDSO, provided over 200 participants with information on a variety of technical and non-technical issues pertaining to the safety, security, and protection of the Nation's dams and related infrastructure.
- Developed technical guidelines such as *Estimating Indirect Economic Consequences for Dam Failure Scenarios*. This document provides information on approaches and methodologies for estimating indirect economic consequences resulting from dam failure or disruption.
- Completed the research project *Assessment and Mitigation of Waterside Attacks on Dams*, which was performed by the University of Kentucky through the National Institute for Hometown Security. The objective of this research project, funded by the DHS Science and Technology Directorate, was to identify and prioritize practical risk-mitigation solutions for water-side threats to dams and gated spillways.

KEY INITIATIVES

Dams Sector partners are implementing numerous protective programs and initiatives to help sustain an effective security posture while addressing emerging risks and enhancing resilience. Key initiatives include the following:

- Increasing awareness of the threat environment across the Dams Sector by identifying and communicating sector-specific threats that take into account physical, cyber, and human elements
- Developing guides and reference documents to manage the risks and support technical transfer, outreach, and training on readiness, response, protection, and recovery issues
- Developing multijurisdictional exercises and regional pilot programs to assess the affects of interdependencies, define effective mitigation strategies, and enhance disaster resilience

PATH FORWARD

The Dams Sector's security and resilience posture will continue to be enhanced through multiple initiatives addressing priority issues. As a result, Dams Sector partners will continue their active collaboration efforts in a number of key areas:

- Support implementation of Executive Order 13636: Improving Critical Infrastructure (EO 13636) and Presidential Policy Directive-21: Critical Infrastructure Security and Resilience (PPD-21)
- Expand sector partnerships and enhance communication and information sharing across all critical infrastructure partners
- Continue to work with sector stakeholders to identify, prioritize, and pursue mission-essential research and development needs
- Implement screening and prioritization efforts to identify critical infrastructure and implement an effective program to characterize critical assets
- Continue DSAT collaborative efforts, including development of onsite and virtual training opportunities for emergency managers and dam safety officials
- Conduct technical seminars and specialty workshops to offer information on fundamental security and resilience concepts for dams, levees, hydropower plants, and related critical infrastructure
- Conduct the Dams Sector Information Sharing Drill annually to provide sector stakeholders the opportunity to evaluate information-sharing mechanisms related to physical threats and cyberthreats



Defense Industrial Base Sector

The Defense Industrial Base (DIB) is the worldwide industrial complex that enables research and development, design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts to meet U.S. military requirements. The DIB partnership consists of U.S. Department of Defense (DOD) components; more than 100,000 DIB companies and their subcontractors who perform under contract to DOD; and companies providing incidental materials and services to DOD. For more information on the sector's vision, goals, and risk-management approach, please see the [Defense Industrial Base Sector Snapshot](#) and the 2010 [Defense Industrial Base Sector-Specific Plan](#).

SELECTED ACCOMPLISHMENTS

Sector partners continue to enhance the DIB Sector's security posture. Accomplishments over the past year include the following:

- Proved instrumental in the DOD response to National Security Staff efforts to revise Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection
- Influenced the development of the Protection mission area within the National Preparedness Framework under Presidential Policy Directive 8: National Preparedness
- Coordinated with the U.S. Department of Homeland Security (DHS) to improve sector information sharing at the local level and integrate owners and operators into information-sharing environments at State and major urban area fusion centers
- Continued to expand the DIB Cybersecurity/Information Assurance program and the DIB Enhanced Cybersecurity Services program
- Maintained an emergency notification system that can reach DIB Sector Coordinating Council (SCC) partners
- Integrating DIB Sector-Specific Agency (SSA) responsibilities into implementation of the DOD Mission Assurance Strategy
- Conducting a regional energy dependency assessment and recommending a dependency analysis methodology that partners may use to improve the resilience of commercial grid infrastructure in support of DIB facilities
- Improving the process for determining and prioritizing the criticality of private-sector DIB assets and creating a national DIB risk profile
- Identifying existing information-sharing portals and pursuing a system that will enable a robust two-way information-sharing capability
- Working to better coordinate DOD, DHS Office of Infrastructure Protection, and U.S. Department of State international initiatives

PATH FORWARD

The sector will take the following steps as it moves forward:

- 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
- Integrate PPD-21 and EO 13636 into DIB Sector planning by contributing to the development of the new *National Infrastructure Protection Plan* and development of a new *DIB Sector-Specific Plan* with revised goals, objectives, and associated implementation actions

KEY INITIATIVES

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

- Organizing DOD implementation of Executive Order 13636: Improving Critical Infrastructure (EO 13636) and Presidential Policy Directive-21: Critical Infrastructure Security and Resilience (PPD-21)

For a complete list of DIB Sector CIPAC members, please visit [Council Members, Critical Infrastructure Partnership Advisory Council](#), available on the DHS Website.



Emergency Services Sector

The Emergency Services Sector (ESS) is 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 affected by disasters (natural or manmade), and aid recovery from

emergency situations. 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. As a primary protector of other critical infrastructure sectors, an attack on ESS capabilities could notably affect the Nation's security, public safety, and morale. For more information on the sector's vision, goals, and risk-management approach, please see the [Emergency Services Sector Snapshot](#) and the 2010 [Emergency Services Sector-Specific Plan](#).

SELECTED ACCOMPLISHMENTS

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

- Developed, published, and distributed the *Emergency Services Sector-Cyber Risk Assessment (ESS-CRA)* as part of the Cybersecurity Assessment and Risk Management Approach methodology. The ESS-CRA is the first ESS-wide assessment that analyzes strategic cyberrisks to ESS infrastructure
- Developed the *Emergency Services Sector Roadmap to Secure Voice and Data Systems*, based on the cyberrisks identified in the ESS-CRA. The roadmap provides a path forward for sector partners looking to further develop their technology security and proposes risk-management responses
- Formed a Pandemic Working Group that was expanded to a Working Group on Medical Countermeasures to focus on a national strategy for protecting the health of emergency services personnel, thereby protecting the capacity of the ESS
- Partnered with the Federal Emergency Management Agency Continuity of Operations Division to develop a Continuity of Operations (COOP) Survey, which will gather an understanding of how ESS incorporates COOP planning into their emergency management operations as identified in *Continuity Guidance Circular 1*
- Developed Fire Service Standing Information Needs to support focused intelligence gathering

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:

- Improving timely, validated, protected, and actionable information-sharing processes and protocols through the ESS Information Sharing Working Group efforts
- Continuing sector-focused collaborative efforts through the Critical Infrastructure Partnership Advisory Council and the sector's national association footprint to identify and promulgate sector-based capacity-building tools, programs, and training
- 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
- Supporting the ESS Cybersecurity Initiative through focused outreach to help ESS partners secure and protect their cyberinfrastructure from a broad range of natural and manmade threats
- Landscaping and promulgating current credentialing and crisis reentry efforts, which support nationwide critical infrastructure resilience activities

PATH FORWARD

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

- Continue outreach to bring awareness to the *Emergency Services Sector Roadmap to Secure Voice and Data Systems*, which helps to identify risk responses for each of the cyber risks identified in the ESS-CRA
- Continue to work collaboratively with the DHS National Cybersecurity Division on continued distribution of the Cyber Risk Assessment, further development of the roadmap, expansion of the Cyber Exercise Program, and information-sharing efforts in order to help promote cybersecurity awareness and information sharing about sector-specific threats
- Mature the Resilience Development Program, which will consist of capacity-building products and expertise focused on the unique needs of the sector. It will be offered to ESS practitioner organizations to provide customized enhancements to their resilience and overall readiness.
- Define a path forward on crisis reentry and access control for public and private emergency responders 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

For a complete list of ESS CIPAC members, please visit [Council Members, Critical Infrastructure Partnership Advisory Council](#), available on the DHS Website.



Energy Sector

The Energy Sector consists of thousands of geographically dispersed electricity, oil, and natural gas assets that are connected by systems and networks. Without a stable energy supply, health and welfare are threatened, and the U.S. economy cannot function. More than 80 percent of the country's energy infrastructure is owned by the private sector, supplying fuels to the transportation industry, electricity to households and businesses, and other sources of energy that are integral to growth and production across the Nation; therefore, collaboration is essential to secure this interdependent infrastructure. Sector public-private partnerships facilitate information sharing regarding threats, vulnerabilities, and protective measures. For more information on the sector's vision, goals, and risk-management approach, please see the [Energy Sector Snapshot](#) and the 2010 [Energy Sector-Specific Plan](#).

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:

- Completed the Electricity Subsector Cybersecurity Capability Maturity Model (C2M2)
- Engaged in the development of Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21) and Executive Order 13636: Improving Critical Infrastructure Cybersecurity (EO 13636)
- Organized sector efforts to respond to evolving cyberthreats.
- Coordinated the Energy Sector emergency response to Superstorm Sandy and other incidents in cooperation with the U.S. Department of Energy (DOE) and the Federal Government
- Held high-level discussions with the U.S. Department of Homeland Security (DHS), DOE, and electricity sector CEOs that focused on cybersecurity and issues identified in the National Infrastructure Advisory Council report, *A Framework for Establishing Critical Infrastructure Resilience Goals*
- Held multiple classified briefings regarding physical security and cybersecurity
- Created a Communications Process Model to enhance the preparedness capability of the oil and natural gas industry through Federal emergency preparedness information sharing and coordination

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:

- Working with DHS to process security clearances
- Continuing high-level engagements between industry and senior government officials
- Working with the Oil and Natural Gas Subsector to identify approaches to enhance communication during energy-related national emergencies
- Collaborating with DHS, the Federal Bureau of Investigation, and others on information sharing
- Working with sector partners on the implementation of PPD-21 and EO 13636
- Cooperating with sector partners to develop and begin implementation of an Oil and Natural Gas Subsector C2M2 to help the sector 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 cybervulnerabilities 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:

- Complete development of the C2M2 process tool for the Oil and Natural Gas Subsector
 - Continue development of the Cyber Incident Management Plan
 - Work with the DHS Office of Science and Technology Policy to progress Energy Sector research and development
 - Continue to lead the implementation of requirements outlined in the Emergency Support Function #12 – Energy Annex, which is intended to facilitate the restoration of damaged energy systems and components when activated by the Secretary of Homeland Security for incidents requiring a coordinated Federal response
- Continue to coordinate Superstorm Sandy After Action efforts
 - Collaborate with the Federal Emergency Management Agency to educate the public regarding “Whole Community” preparedness efforts for hurricane season
 - Continue with efforts to develop physical security, cybersecurity, reliability, and resilience metrics that can be used to track and report on Energy Sector activities and advances
 - Continue to coordinate with the Joint Oil and Natural Gas, Chemical, and Pipeline Working Groups



Financial Services Sector

The Financial Services (FS) Sector is essential to facilitating world economic activity. The institutions, markets, and infrastructure that make up the U.S. financial system provide essential services to the U.S. and global economies—helping to allocate funds from savers to borrowers, allowing households and businesses to plan for the future and manage their risks over time, and facilitating the enormous volume of financial transactions necessary to support real economic activity and employment on a daily basis. The sector faces a wide range of potential risks, including large-scale power outages, natural disasters, and cyberattacks. For more information on the sector’s vision, goals, and risk-management approach, please see the [Financial Services Sector Snapshot](#) and the 2010 [Financial Services Sector-Specific Plan](#).

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 cyberattackers
- 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 FS Sector through a series of briefings
- Conducted research under the previously completed memorandum of understanding on cybersecurity research developed in conjunction with the White House, U.S. Department of Homeland Security (DHS), 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*

PATH FORWARD

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

- Enhance the quality and timing of information sharing and coordination
- Integrate the sector’s Threat Analysis Tool into risk-management and contingency plans
- Conduct exercises and training targeted to address identified issues
- Provide expert advice on national cybersecurity policy issues to senior Federal, State, and local officials; and coordinate efforts internationally
- Address supply chain risks and financial top-level domain concerns
- Ensure continuity of leadership and expand participation of private-sector partners, including through expanded Financial Services Sector Coordinating Council (FSSCC) membership
- Continue senior leadership meetings between the FSSCC and the Financial and Banking Information Infrastructure Committee to identify ways of addressing issues of mutual concern
- Improve identity proofing through the joint government-FSSCC pilot effort, Financial Institutions–Verifying Identity Credentials Services
- Invest in research and development

For a complete list of FS Sector CIPAC members, please visit [Council Members, Critical Infrastructure Partnership Advisory Council](#), available on the DHS Website.



Food and Agriculture Sector

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 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. For more information on the sector's vision, goals, and risk-management approach, please see the [Food and Agriculture Sector Snapshot](#), the 2010 [Food and Agriculture Sector-Specific Plan](#), and the 2010-2011 [Food and Agriculture Sector Annual Report](#).

SELECTED ACCOMPLISHMENTS

Sector partners continue to maintain and enhance the protective security of the FA Sector. Selected accomplishments over the past year include the following:

- Established a State, local, tribal, and territorial co-chair and vice chair for the Government Coordinating Council (GCC)
- Approved the following Information Sharing Standard Operating Procedures for the FA Sector: Application, Validation, and Vetting into Web-based Information Sharing; Routine Communication and Coordination; Incident Communication and Coordination; Alerts, Warnings, and Notification; Suspicious Activity Reporting; and Data Management
- Partnered with the Nuclear Reactor, Materials, and Waste Sector to conduct an information-sharing/communications workshop in March 2013. A follow-on tabletop exercise was held in September 2013
- Participated in the Extension Disaster Education Network Agrosecurity Symposium: Building National Networks and Partnerships in April 2013 and provided an overview of sector activities mapped to core capabilities established to support the National Preparedness Goal
- Convened a joint regional workshop through the Multistate Partnership for Security in Agriculture and the Southern Agriculture and Animal Disaster Response Alliance in April 2013 that resulted in a progress review and gap analysis for continued enhancements to sector security and resilience
- Convened a "Criticality in the Food and Agriculture Sector Workshop" in December 2012 to discuss improvements to the process for prioritization of the FA Sector critical infrastructure and ongoing efforts to reduce risk across the sector

KEY INITIATIVES

Numerous security programs are contributing to a more secure FA Sector. Key initiatives 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
- Promoting and using research capabilities, sector knowledge, and existing tools and programs to strengthen sector resilience

PATH FORWARD

To improve protection of the FA Sector, Sector-Specific Agencies, and sector partners will take the following steps to move forward:

- Work on the revisions to the FA Sector Criteria for the Fiscal Year 2015 National Critical Infrastructure Prioritization Program Data Call
- Continue to work with sector partners to prioritize activities and leverage resources to ensure a secure and resilient FA Sector with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from threats and hazards of greatest risk

For a complete list of FA Sector CIPAC members, please visit [Council Members, Critical Infrastructure Partnership Advisory Council](#), available on the DHS Website.



Government Facilities Sector

The Government Facilities Sector (GFS) includes a wide variety of facilities located 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. For more information on the sector's vision, goals, and risk-management approach, please see the [Government Facilities Sector Snapshot](#).

SELECTED ACCOMPLISHMENTS

Sector partners continue to maintain and enhance the security of the GFS. Accomplishments over the past year include the following:

- Introduced the new Federal Protective Service (FPS) policy on prohibited items at Federal facilities
- Held a GFS Government Coordinating Council (GCC) conference call to discuss the security procedures FPS implemented at Level 4 buildings across the country after the Boston Marathon bombing
- Met with senior representatives from the Prince George's County Police Department (PGPD) who requested help with using a Federal Government resource in the county. Two members of the PGPD joined the GFS GCC.
- 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

Numerous security programs are contributing to a more secure GFS. Key initiatives 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 comply with a range of physical security standards, including the Interagency Security Committee 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 Mega Centers
- 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:

- Develop or coordinate a sector-wide risk assessment
- Enhance Information Technology (IT) systems and related operations to include systems and technologies for Mega Centers and other IT infrastructure
- 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 *Government Facilities Sector-Specific Plan*
- Expand available metrics to measure progress toward achieving GFS goals



Healthcare and Public Health Sector

The Healthcare and Public Health (HPH) Sector constitutes approximately 17 percent of the gross national product and is extremely important to the U.S. economy and the well-being of the Nation's citizens. Protection of critical infrastructure in the HPH Sector is essential to maintaining a resilient Nation, as it protects all sectors from hazards including infectious disease outbreaks, terrorism, and natural disasters. Privately owned and operated organizations compose approximately 85 percent of the sector, and the public health component is carried out largely by government agencies. Therefore, collaboration and information sharing among public- and private-sector entities are critical to maintaining a resilient sector. For more information on the sector's vision, goals, and risk-management approach, please see the [Healthcare and Public Health Sector Snapshot](#) and the 2010 [Healthcare and Public Health Sector-Specific Plan](#).

SELECTED ACCOMPLISHMENTS

Sector partners continue to maintain and enhance the resilience of the HPH Sector. Accomplishments over the past year include the following:

- Collaborated with the Critical Infrastructure Protection (CIP) Program on Critical Asset Identification Process (CAIP) efforts, reviewing submittals and confirming the currency of information as they identify the regional-level (Level 4) and State/local-level (Level 5) HPH critical infrastructure
- Prepared and delivered quarterly classified briefings in collaboration with the U.S. Department of Health and Human Services Office of Security and Strategic Information and the U.S. Department of Homeland Security (DHS) Office of Health Affairs
- Continued hosting a quarterly Webinar series to educate partners on a variety of topics related to HPH Sector critical infrastructure security and resilience
- Increased membership of the Homeland Security Information Network (HSIN)–HPH portal through trade association outreach, HSIN portal marketing materials, and the new Webinar series, enabling the sector to provide threat and risk information to hundreds more stakeholders
- Utilized HSIN–HPH during the response to Superstorm Sandy, the Boston Marathon bombings, and the Oklahoma City-area tornadoes, which enabled the HPH CIP Program to populate a site with incident-specific information, including mapping products that highlighted potential affects to infrastructure of concern and a discussion board for sharing information

- Met with the Risk Management, Cybersecurity, Information Sharing, and Research and Development joint working groups to develop ideas and products that provide specific benefits to the sector. Recent products include a cybersecurity checklist and a document outlining funding opportunities for critical infrastructure security and resilience.

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 cybersystems. Key initiatives include the following:

- Conducting four classified briefings per year for stakeholders who possess a Secret-level clearance or higher, conducting unclassified briefings for larger audiences, and presenting at various conferences to inform attendees about the CIP Program and topics related to critical infrastructure security and resilience
- Funding security clearances for State health department personnel, including 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, actionable information related to steady-state and emergency response scenarios
- Disseminating a biweekly newsletter to all users highlighting articles and reports focused on critical infrastructure security and resilience added to the HSIN–HPH portal document library
- Conducting monthly Sector Coordinating Council/ Government Coordinating Council calls or sending emails to alert the sector to noteworthy events

- 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 significantly affect public health
- Collaborating with the U.S. Department of Energy to implement the Power Monitoring Pilot Program, which will install devices on a voluntary basis in critical HPH facilities throughout the Nation to constantly monitor and provide real-time communication on the facilities' power status
- Developing and piloting an approach to assess risks for each HPH critical asset identified in the CAIP
- Working with DHS and other Sector partners to implement Presidential Policy Directive 21: Critical Infrastructure Security and Resilience and Executive Order 13636: Improving Critical Infrastructure

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:

- Increase participation from partners at all levels of government and in 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 steady-state and incident response
- Collaborate with HPH Sector partners to continue the risk-management process for the sector
- Coordinate outreach and information sharing with facilities identified through CAIP with DHS and other Federal, State, and local partners
- Collaborate with HPH SCC Ad Hoc Active Shooter Committee members, DHS, and others to develop a template and video on how hospitals should respond to active shooter incidents



Information Technology Sector

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. For more information on the sector's vision, goals, and risk-management approach, please see the [Information Technology Sector Snapshot](#) and the 2010 [Information Technology Sector-Specific Plan](#).

SELECTED ACCOMPLISHMENTS

Sector partners continue to maintain and enhance the resilience and security posture of the IT Sector. Accomplishments over the past year include the following:

- Completed the updated *IT Sector Identity Management and Associated Trust Support Services Risk Assessment* and 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 infrastructure by considering changes since the release of the *Provide Domain Name Resolution Services* critical function risk profile in the 2009 *Information Technology Sector Baseline Risk Assessment*
- 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 U.S. Department of Homeland Security Cyber Ecosystem framework and *Blueprint for a Secure Cyber Future* strategy

KEY INITIATIVES

Key initiatives within the IT Sector include the following:

- 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 infrastructure; identify management activities in response to those risks; and update the risk profile
- Facilitating progress toward 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, 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 that supply chain risks are effectively managed by documenting and sharing supply chain risk-management practices through multiple forums and initiatives, including the *Draft NIST Interagency Report 7622: Supply Chain Risk Management Practices for Federal Information Systems*

PATH FORWARD

Effective collaboration between the public and private sectors has driven significant progress in the past. Throughout 2013 and 2014, 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
- Reinvigorate the IT Sector Supply Chain Risk Management Working Group to determine goals and objectives for IT Sector supply chain security
- Engage with government-established Interagency Tasks Forces to implement Executive Order 13636: Improving Critical Infrastructure and Presidential Policy Directive 21: Critical Infrastructure Security and Resilience
- Foster improved real-time, bidirectional control systems and cybersystems information sharing to achieve a common operating picture across the critical infrastructure community
- Collaborate with industry on cybersecurity policy planning efforts and/or co-develop policies to achieve mutually beneficial outputs (e.g., influencing acquisition policy)



Nuclear Reactors, Materials, and Waste Sector

The Nuclear Reactors, Materials, and Waste Sector (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. For more information on the sector's vision, goals, and risk-management approach, please see the [Nuclear Sector Snapshot](#) and the 2010 [Nuclear Sector-Specific Plan](#).

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:

- Planned and conducted Integrated Response Exercises at two nuclear power plants in coordination with the Federal Bureau of Investigation (FBI), the Nuclear Regulatory Commission (NRC), and private-sector partners:
 - Surry Power Station in Surry, Virginia: Seventeen local, State, and Federal law enforcement agencies participated in the December 10, 2012, Tabletop Exercise and twelve participated in the Limited Exercise on December 13, 2012.
 - Davis-Besse Nuclear Power Station in Oak Harbor, Ohio: Fourteen local, State, and Federal law enforcement agencies participated in the June 19, 2013 Tabletop Exercise and ten participated in the Limited Exercise on June 21, 2013.
- Conducted a cross-sector planning workshop including the Nuclear and Food & Agriculture Sectors focused on information sharing and communication protocols for a major radiological contamination event. Representatives from seven Federal agencies and three States participated, in addition to the Nuclear and Food & Agriculture Sector Coordinating Councils
- Coordinated the following efforts through the Nuclear Sector Radioisotopes Subcouncil:
 - Maintained awareness and active engagement with continuing low-level waste disposal and transportation of radioactive sources efforts
 - Promoted awareness and coordination of policies, strategies, plans, and measures that enhance the physical security, emergency preparedness, and resilience of the Nation's radioisotopes under the auspices of the *National Infrastructure Protection Plan*
- Coordinated the following efforts through the Nuclear Sector Joint Cyber Subcouncil:
 - Promoted the *Roadmap to Enhance Cyber Systems Security in the Nuclear Sector* and the Nuclear Sector Annex to the National Cyber Incident Response Plan
 - Hosted briefings with the Industrial Control Systems Cyber Emergency Response Team
- Coordinated the following efforts through the Nuclear Sector Joint Non-Power Reactor Subcouncil:
 - Promoted cybersecurity measures in collaboration with the NRC
- Organized and hosted classified information-sharing sessions with industry partners
- Coordinated with industry and Federal partners to ensure the timely, secure shipment of radiopharmaceuticals to medical facilities during a National Special Security Event

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 include the following:

- Facilitating additional voluntary security enhancements, such as the Research and Test Reactors Voluntary Security Enhancement Project and Cesium Chloride Irradiator In-Device Delay Program
- Conducting Integrated Response Exercises and other emergency preparedness activities
- Conducting FBI outreach visits to select facilities housing risk-significant radioactive materials and special nuclear material

PATH FORWARD

The Nuclear Sector's robust security posture will continue to be enhanced in a number of key areas, including integrated response capabilities, cybersecurity, ensuring safe and secure storage or disposal for commercial-sealed sources, and increasing the resilience of the radioisotopes supply chain. As a result, the sector will take the following steps:

- Support implementation of Presidential Policy Directive 21: Critical Infrastructure Security and Resilience and Executive Order 13636: Improving Critical Infrastructure
- Move forward with development of the next-generation Integrated Response Planning Program
- 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 coordinate on cybersecurity issues affecting the Nuclear Sector
- Support radioisotopes supply chain resilience by participating in interagency efforts to enhance supplies of key radioisotopes, such as Molybdenum-99



Transportation Systems Sector

The Transportation Systems Sector is a vast, open network of interdependent systems that quickly, safely, and securely move people and goods through the country and overseas. The sector is critical to the public health, safety, security, and economic well-being of our Nation. It consists of six interconnected subsectors or modes: aviation, freight rail, highway & motor carriers, maritime, mass transit & passenger rail, and pipelines. For more information on the sector's vision, goals, and risk-management approach, please see the [Transportation Systems Sector Snapshot](#) and the [Transportation Systems Sector-Specific Plan](#).

SELECTED ACCOMPLISHMENTS

The Transportation Systems Sector has made many improvements to its security posture. The sector's accomplishments over the past year include the following:

- Implemented risk-based security enhancements at airports, including TSA Pre✓™, to focus on high-risk screening and expedited travel for those considered 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
- 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 to assess the effectiveness of security measures in over 175 ports of nations conducting maritime trade with the United States
- 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*
- Developed and contributed to the *National Infrastructure Protection Plan (NIPP)*, *Transportation Systems Sector-Specific Plan*, and other policy products, including those pertaining to Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21) and Executive Order 13636: Improving Critical Infrastructure Cybersecurity (EO 13636)
- Continued updating the *Maritime Modal Annex of the Transportation Systems Sector-Specific Plan*
- Provided input to the *National Strategy for Transportation Security*, the *National Strategy for Aviation Security*, the *National Strategy for Maritime Security*, Presidential Policy Directive 18: Maritime Security, and products related to the Homeland Infrastructure Threat and Risk Analysis Center
- Participated in meetings of the other Government Coordinating Councils, including but not limited to, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Nuclear, and State, Local, Tribal, and Territorial

KEY INITIATIVES

The Transportation Systems Sector is undertaking a variety of initiatives to enhance its protection and resilience, including 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 the following voluntary and regulatory risk-management initiatives to secure its critical infrastructure and resources:

- Engage in supporting the implementation of PPD-21 and EO 13636
- Continue to update the *Transportation Systems Sector-Specific Plan* and its annexes
- Continue to coordinate with security partners to implement the mission, goals, and objectives of the NIPP and the *Transportation Systems Sector-Specific Plan*
- Engage sector and transportation owners and operators in strategic partnerships to develop efficient and effective security solutions; increase cybersecurity awareness and understanding; and encourage the use of tools, audits, and assessments
- Engage the State, Local, Tribal, and Territorial Government Coordinating Council (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 security and resilience objectives with overall U.S. foreign policy
- Promote awareness and education opportunities for critical infrastructure security and resilience
- 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

For a complete list of Transportation Systems Sector CIPAC members, please visit [Council Members, Critical Infrastructure Partnership Advisory Council](#), available on the DHS Website.



Water Sector

The Water Sector (Water and Wastewater Systems) includes more than 160,000 public drinking water systems and approximately 16,000 publicly owned 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. 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 coordinated partnerships assist drinking water and wastewater utilities to increase resilience and prepare to prevent, detect, respond to, and recover from all hazards. For more information on the sector's vision, goals, and risk-management approach, please see the [Water Sector Snapshot](#) and the 2010 [Water Sector-Specific Plan](#).

SELECTED ACCOMPLISHMENTS

Sector partners continue to maintain and enhance the security posture of the Water Sector. Accomplishments over the past year include the following:

- Completed the deployment of, commenced analysis of, and began developing a publication of results from five U.S. Environmental Protection Agency Water Security Initiative pilots
- Increased the number of Water and Wastewater Agency Response Networks (WARNs) to 49 States, the National Capital Region, and 2 Canadian Provinces
- Completed and released the Water Health and Economic Analysis Tool 2.0, which now includes assessment and consequence analysis for wastewater hazardous gas releases
- Developed *Containment and Disposal of Large Amounts of Contaminated Water: A Support Guide for Water Utilities*
- Developed *Business Continuity Planning for Water Utilities: Guidance Document* and associated training and outreach
- Conducted the fourth Full Scale Laboratory Exercise in EPA Regions 4, 5, and 6
- Expanded the Water Laboratory Alliance Members to 139 laboratories across 48 States
- Conducted 7 water-specific training courses on the Incident Command System and the National Incident Management System
- Expanded the Water Information Sharing and Analysis Center (WaterISAC) with a significant increase in membership (to 11,700 individuals) and in products and services, such as Webcasts and threat briefings
- Completed J-100 and Contamination Warning System Critical Infrastructure Partnership Advisory Council (CIPAC) Workgroups and issued reports for each
- Issued the WARN Superstorm Sandy After Action Reports
- Initiated the development of cybersecurity guidance for the Water Sector
- Updated the *Roadmap to a Secure & Resilient Water Sector*
- Participated in implementation of Presidential Policy Directive 21: Critical Infrastructure and Resilience and Executive Order 13636: Improving Critical Infrastructure.
- Leveraged the CIPAC framework to develop sector priorities, build partnerships, and increase collaboration among public and private-sector stakeholders

KEY INITIATIVES

The Water Sector continues to work collaboratively to minimize the obstacles that owners and operators may face while they are implementing security programs. Key initiatives include the following:

- Advancing the development of sector-specific cybersecurity resources
- Raising awareness of the Water Sector as a lifeline sector and recognize the priority status of its needs and capabilities
- Supporting the development and deployment of tools, training, and other assistance to enhance preparedness and resilience

PATH FORWARD

The Water Sector plans to implement various programs to enhance the security and resilience of its assets, including the following:

- Develop advanced cybersecurity guidance, practices, and tools that are sustainable, effective, and implementable for utilities of all sizes and types
- Conduct State and local exercises that improve understanding of Water Sector interdependencies and the affects of loss of service during a disaster
- Develop a tool consistent with the American National Standards Institute/American Water Works Association J100-10 standard to help utilities update all-hazards risk assessments, and then leverage the assessments to update emergency response and risk-management plans; perform after action analyses; and incorporate lessons learned following an event
- Increase participation in the WaterISAC and further leverage the center to disseminate security and resilience information to utilities and government agencies
- Examine Federal Emergency Management Agency assistance criteria for applicability to the Water Sector
- Build stronger engagement with the State, Local, Tribal, and Territorial Government Coordinating Council to raise awareness at the State and local levels
- Perform after action analyses after large events to highlight economic implications for the Water Sector
- Encourage utilities to develop a risk profile using both cyberrisk and physical risk tools
- Examine design standards and climate change adaptation strategies to identify “no regret” upgrades that offer multiple types of benefits

Page intentionally left blank

Page intentionally left blank



Homeland
Security