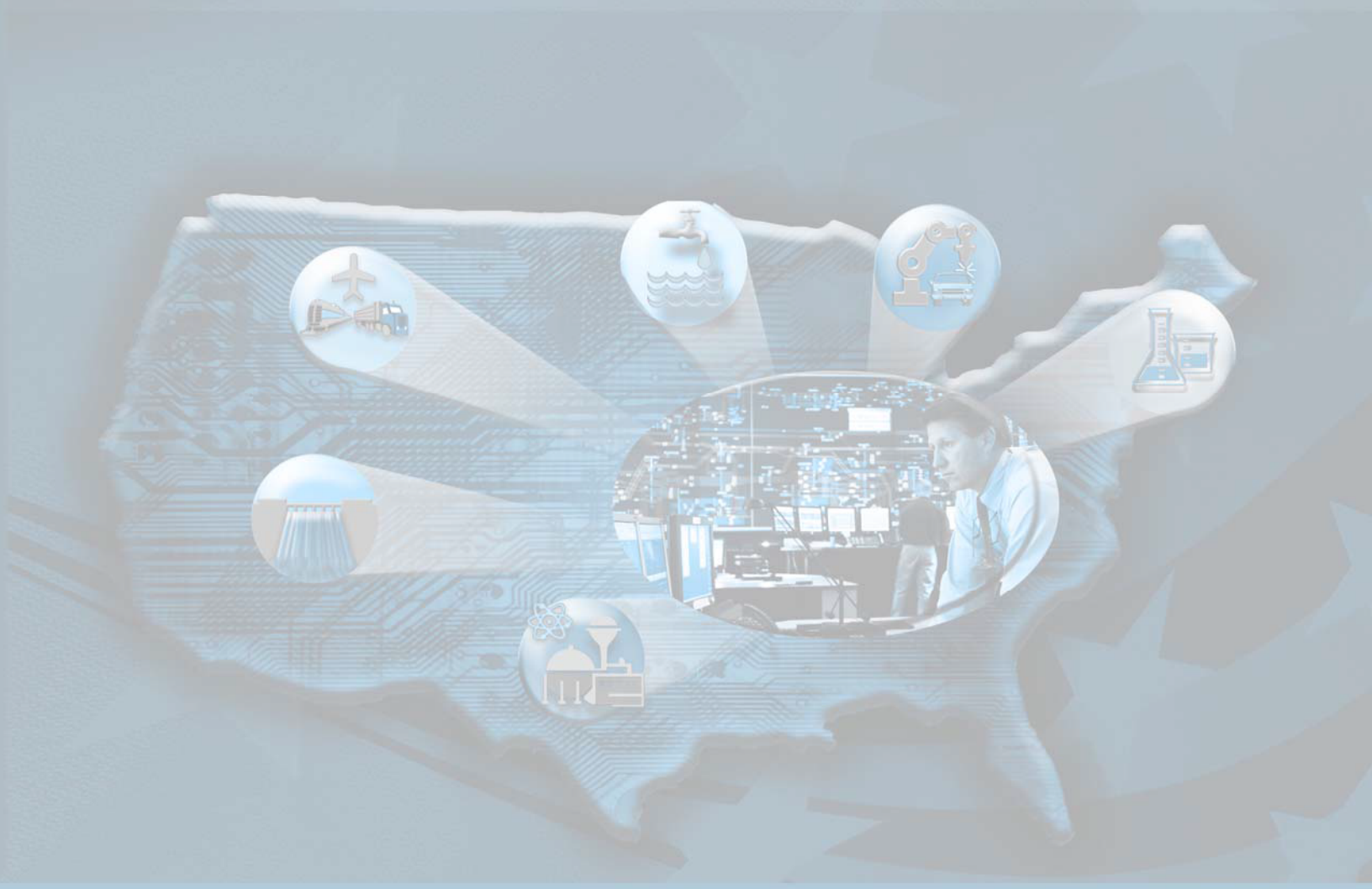
Strategy for Securing Control Systems

Coordinating and Guiding Federal, State and Private Sector Initiatives

October 2009

Homeland Security



STRATEGY FOR SECURING CONTROL SYSTEMS

CONTENTS

ACRONYMS

ACC	American Chemistry Council
ASDSO	Association of State Dam Safety Officials
CERT/CC	Carnegie Mellon's CERT Coordination Center
ChemITC	Chemical Information Technology Center
CIA	Central Intelligence Agency
CIKR	Critical Infrastructure and Key Resource
CIPAC	Critical Infrastructure Partnership; Advisory Council
CSCSWG	Cross-Sector Cyber Security Working Group
CS&C	Cyber Security and Communication (Office of)
CSSP	Control Systems Security Program
CSVA	Cyber Security Vulnerability Assessment Tool
CS2SAT	Control Systems Cyber Security Self Assessment Tool
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DOD	Department of Defense
DOE	Department of Energy
FBI	Federal Bureau of Investigations
Federal Partners	Federal Control Systems Security Working Group
FERC	Federal Energy Regulatory Commission
GAO	Government Accountability Office
GCC	Government Coordinating Councils
GFIRST	Government First Incident Response Security Teams
HITRAC	Homeland Infrastructure Threat and Risk Assessment Center
HSIN	Homeland Security Information Network
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ICSJWG	Industrial Control Systems Joint Working Group
ISAC	Information Sharing and Analysis Center
IEC	International Electrotechnical Commission
ISA	Instrumentation, Systems, and Automation Society
IT	Information Technology
MS-ISAC	Multi-State Information Sharing and Analysis Center
NCRCG	National Cyber Response Coordination Group
NCSD	National Cyber Security Division
NEI	Nuclear Energy Institute
NERC	North American Electric Reliability Corporation
NIAC	National Infrastructure Advisory Council
NICC	National Infrastructure Coordinating Center
NIST	National Institute of Standards and Technology
NIPP	National Infrastructure Protection Plan
NOC	National Operations Center
NPPD	National Protection and Programs Directorate

NRC	National Research Council
PCIS	Partnership for Critical Infrastructure Security
PCSF	Process Control Systems Forum
POD	Partnership and Outreach Division
PSA	Protective Security Advisor
R&D	Research and Development
RBPS	Risk Based Performance Standards
SAR	Sector Annual Report
SCADA	Supervisory Control and Data Acquisition
SCC	Sector Coordinating Council
SME	Subject Matter Experts
SSA	Sector Specific Agencies
SSP	Sector Specific Plans
S&T	Science and Technology (a DHS Directorate)
US-CERT	United States Computer Emergency Readiness Team
WERF	Water Environment Research Foundation

EXECUTIVE SUMMARY

Our nation depends on the continuous and effective performance of a vast and interconnected critical infrastructure to sustain our modern way of life. This infrastructure, the majority of which is owned by the private sector, is comprised of critical infrastructure and key resource (CIKR) sectors as identified in the National Infrastructure Protection Plan (NIPP).[1] These sectors include Energy, Chemical, Banking and Finance, Water Treatment, Postal and Shipping, Agriculture and Food, Defense Industrial Base, Commercial Nuclear Reactors, and many more (see Section 4.2).

> "The ability to protect the critical infrastructure and key resources (CIKR) of the United States is vital to our national security, public health and safety, economic vitality, and way of life."
>
> *National Infrastructure Protection Plan*

Although each of the critical infrastructure industries is vastly different, they are all dependent on control systems to monitor, control, and safeguard their vital processes. As such, the U.S. Department of Homeland Security (DHS) has recognized that the protection and security of control systems is essential to the Nation's overarching security and economy. Industrial control systems perform various functions and vary in lifecycle duration throughout the nation's critical infrastructure. Many of the industrial control systems used today were designed for operability and reliability during an era when security received low priority. In today's open communications environment, industrial control systems are now highly network-based and use common standards for communication protocols. CIKR asset owners and operators have gained immediate benefits by extending the connectivity of their industrial control systems. However, this connectivity exposes network assets to cyber infiltration and subsequent manipulation of sensitive operations. Furthermore, increasingly sophisticated cyber attack tools can exploit vulnerabilities in commercial industrial control system components, telecommunication methods, and common operating systems found in modern industrial control systems.

The Strategy for Securing Control Systems (subsequently referred to as the *Strategy*) has been created by the Department's National Cyber Security Division (NCSD) as part of the overall mission to coordinate and lead efforts to improve control systems security in the nation's critical infrastructures. The *Strategy* also addresses concerns outlined in the September 2007 Government Accountability Office (GAO) report entitled "*Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*."[2] In this report, GAO asserts that an overarching strategy was needed to guide and coordinate the efforts of various private and public organizations that had created initiatives for securing control systems.

The primary goal of the *Strategy* is to build a long-term common vision where effective risk management of control systems security can be realized through successful coordination efforts. Implementing the *Strategy* will create a common vision with respect to participation, information sharing, coalition building, and leadership activities. Its implementation will improve coordination among relevant stakeholders within government and private-sector, thereby reducing cybersecurity risks to control systems.

The *Strategy* leverages the risk management framework and partnership model described in the NIPP, by providing a path forward for coordination among CIKR stakeholders, government, and industry associations within the NIPP public-private sector partnership. Multiple programs and activities within the sponsorship and participation of the NIPP public-private partnerships, and independently in industry, are increasing the opportunities and need for coordinated actions. The "coordination landscape" is defined by the *Strategy* and includes activities which will enhance the nation's security posture. Coordination mechanisms for critical

1. "National Infrastructure Protection Plan," Department of Homeland Security, 2006, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.
2. GAO-07-1036, "Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain," September 2007.

infrastructure protection have been created or enhanced by national strategies, policies, and plans such as the NIPP. These mechanisms include the Critical Infrastructure Partnership Advisory Council (CIPAC), which is an enabler of public-private collaboration and partnership coordination around critical infrastructure protection issues among a key set of vetted participants, the Federal Control Systems Working Group (Federal Partners) hosted by the NCSD, and private sector industry organizations, academia, standards bodies, and Information Sharing and Analysis Centers (ISACs). This same landscape approximates the breadth and depth of resources committed to address control systems security.

The overarching control systems security *Strategy*, established to coordinate federal, state, and private sector initiatives, has two principal components: (1) a new CIPAC entity known as the Industrial Control Systems Joint Working Group (ICSJWG), and (2) an expanded Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), managed by the Control Systems Security Program (CSSP), that provides recognized cyber incident response and analysis capabilities in conjunction with the United States Computer Emergency Readiness Team (US-CERT).

The ICSJWG is comprised of two subgroups, one for coordination with government stakeholders and the other for private sector stakeholders and partnerships. The ICSJWG coordinates and builds upon the NIPP partnership framework for control systems security efforts by leveraging activities sponsored by members of the Government Coordinating Councils (GCCs) and/or Sector Coordinating Councils (SCCs).

The ICS-CERT provides a control system security focus in collaboration with US-CERT and the private sector critical infrastructure by expanding the technical and response capabilities and coordination for situational awareness, incident response, and vulnerability management. The focus on control systems cybersecurity provides a direct path for coordination of US-CERT activities with the stakeholders; recognizing that control system security issues are unique.

These two strategic components give DHS the tools to lead coordination activities and accomplish and measure the progress for risk reduction to fulfill its mission responsibilities under the NIPP.

As the federal government's lead agency in cybersecurity coordination and preparedness,[3] DHS will implement the strategy leveraging the NCSD CSSP. In addition, ICSJWG and ICS-CERT will serve as the mechanisms for the overall coordination of control systems security efforts within the framework established and operating under the NIPP.

3. *National Strategy to Secure Cyberspace*, The White House, February 2003, http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf , Website visited June 12, 2009.

1. INTRODUCTION

As the lead federal agency involved in cybersecurity for CIKR, NCSD led development of the *Strategy*, which focuses on the vision and elements for coordinating activities to improve control systems security in the nation's critical infrastructures. Developed within the framework of the NIPP (see Footnote 1), the *Strategy* addresses GAO recommendations (see footnote 2). DHS has authorities that support the *Strategy* as described in Appendix A.

1.1 The Coordination Challenge

DHS recognizes the need to lead and coordinate ongoing efforts to secure control systems. National policy initiatives, Congressional directives, and private sector efforts have increased attention on securing control systems. These initiatives endeavor to improve the security end state of CIKR, but they often reflect agency or sector-specific goals and objectives without a common approach or measure.

The *Strategy* proposes a common vision for sector participation, information sharing, coalition building, and leadership in order to guide stakeholder activities and improve overall coordination. The *Strategy* enables DHS and other stakeholders to coordinate efforts by participating in effective partnerships and developing strategies for improving security. By participating in and supporting this *Strategy*, partnering organizations will develop a shared vision that will benefit both government and private-sector stakeholders.

Effectively and efficiently securing the nation's critical infrastructure control systems from cyber attack will require extensive coordination and participation of both public and private sector security entities. Government and private sector partners will bring a wide range of core competencies and perspectives that add value to the partnership and enable each partner to fulfill its mission. Some benefits of systematic coordination include:

- Opportunities to incorporate specific control systems activities into federal, state, and local security program design and investment
- More timely and accurate dissemination of information on sector CIKR threats and vulnerabilities, recommended practices, assessment methodologies, and other information to help assess and manage risk
- Improved information sharing between stakeholders through relationship building and establishing trust
- Improved communication networks resulting in greater impact and reach of security partner efforts to government agencies, the public, and others
- Improved accuracy and relevance to the type of environment (e.g., voluntary, regulatory) through which sector security is promoted
- Addressing gaps and avoiding duplication of effort

The challenge is to define and implement an effective coordinating mechanism to achieve these benefits and value for the stakeholders primarily with voluntary participation and within an economic business case.

Case Study – Benefits of Coordination
The DHS NCSD Control Systems Security Program and the DOE National SCADA Testbed are two federally funded programs focused on control systems security. These programs leverage expertise, information, and outreach to achieve common goals and objectives, to the benefit of the private sector and government.

1.2 Strategy Overview

The following sections provide the context and outline of the *Strategy*.

- *Purpose, Scope, and Methodology*. Coordination is recognized as a key objective in all security activities derived from national strategies, policy guidance, and plans. The two principal strategy elements provide overall coordination of control systems security activities and are consistent with guidance and implementation of these documents.

- *The Strategy*. The vision of the *Strategy* is to successfully manage risk in critical infrastructures through effective coordination of control systems security activities. The implementation of the *Strategy* to achieve this vision utilizes the framework of the NIPP, which provides the legal and operational mechanisms to coordinate control systems security activities among federal, state, local, and private sector stakeholders. The roles and responsibilities of stakeholders and the associated coordinating mechanisms within this framework are presented.

- *The Industrial Control Systems Joint Working Group (ICSJWG) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).* These two elements of the *Strategy* are introduced as essential elements to implement overall coordination within the NIPP partnership framework. The ICSJWG provides broad coordination of control systems security activities across all stakeholders. Specific activities are described that implement these elements utilizing the resources and authorities of the NIPP. The ICS-CERT addresses the security, threat, and awareness issues unique to control systems and provides a means to share information across all CIKR.

2. PURPOSE, SCOPE, AND METHODOLOGY

The *Strategy* leverages existing efforts and coordination mechanisms to improve the security of control systems. It is the result of two years of collaboration among Federal Partners Working Group, Cross-Sector Cyber Security Working Group (CSCSWG), Process Control Systems Forum Vendor Working Group, and DHS. DHS will have the primary responsibility for implementing the *Strategy*.

2.1 Purpose of the Strategy

DHS developed the *Strategy* to address specific shortfalls and reduce the risk of multiple organizations conducting duplicative work in control systems security, which could lead to missed opportunities to fulfill their critical missions and generate gaps in securing the nation's infrastructure.

To this end, the *Strategy* will:

- Leverage the partnership models for government (federal, state, and local), private sector, and other established entities to coordinate cross-sector efforts to secure CIKR control systems.
- Acknowledge and enhance specific efforts and recommendations of other groups chartered to assess the issues and challenges with control system security.
- Provide improved information sharing with the public and private sectors.
- Guide DHS in scoping and prioritizing its programs within the context of other agency and industry efforts and assessing the performance and sufficiency of available resources to meet its commitments.
- Implement enhanced or expanded awareness and engagement for NCSD to achieve overall coordination of efforts.

2.1.1 NIPP and Other Efforts

As the most significant national effort to coordinate protection initiatives across CIKR, the NIPP partnership framework provides a collaborative framework for establishing priorities, goals, and measures specific to control systems security issues.

The significance of the NIPP to the development and implementation of the *Strategy* is that its key elements, the Risk Management Framework and Government-Private Sector Partnership framework, establish a high-level framework that will serve as both the structure and a driver for coordination and guidance efforts.

For example, DHS currently recognizes the Partnership for Critical Infrastructure Security (PCIS) as the NIPP partnership framework 's Private Sector Cross-Sector Council—an organization that can coordinate cross-sector initiatives that promote public and private efforts to help ensure secure, safe, and reliable critical infrastructure services. Operating in that capacity, PCIS focuses primarily on cross-sector policy, strategy, and interdependency issues affecting the critical infrastructure sectors. Also, as part of the NIPP partnership framework, SCCs provide input to DHS, sector-specific agencies, and private sector asset owners and operators. These efforts make up a portion of the coordinated efforts to engage and empower NIPP stakeholders that implement control systems security activities. One of the challenges for the *Strategy* within the context of the NIPP sector partnerships framework is the level of voluntary participation and trusted relationships needed to have effective communications and information sharing.

2.1.2 Historical Origins and Drivers

Since 2003, several strategies, plans, and advisories (summarized in Table 2-1) have shaped federal activities to improve the security of control systems. Federal agencies, including DHS, the Department of Energy (DOE), and the Department of Defense (DOD) also have multiple initiatives underway. While many of these efforts have improved control systems security, concerns have been raised regarding coordination across all sectors. In addition, the private sector may not know how to effectively engage and benefit from these programs without clear coordination of purpose and benefits.

Table 2-1. Timeline of policies, advisories, and plans supporting control systems security.

Document	Author	Release Date	Type	Summary
National Strategy to Secure Cyberspace	Presidential Directive	2003	Policy	Provides policy direction to DHS and federal agencies on cybersecurity, including control systems. Identifies DHS as the lead agency in this effort.
HSPD-7	Presidential Directive	2003	Policy	Directs DHS, in coordination with other sector-specific agencies, to prepare a national plan to protect the infrastructure to include coordination and participation with the private sector.
Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems	GAO	2004	Advisory	Recommends DHS develop and implement a strategy to coordinate efforts to meet challenges associated with securing control systems and current efforts for both the federal and private sector
National Infrastructure Protection Plan	DHS	2006	Plan	Provides the overarching planning process and structure for security partnerships and federal/private sector response to protect critical infrastructure.
Sector Specific Plans	SSA	2007	Plan	All Sector Specific Agencies (SSAs) in coordination with SCCs were directed to complete plans within the NIPP partnership framework by 2006. These provide high level assessment, goals, and objectives for infrastructure protection.
Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain	GAO	2007	Advisory	Recommends DHS develop a coordination strategy for public and private sectors and process for improving information sharing
Academic: • Toward a Safer and More Secure Cyberspace	NRC	2007	Advisory	The National Research Council (NRC) conducted a study on research priorities for securing cyberspace. Control systems issues were included in their scope.
Sector-Specific Roadmaps/Strategies: • Energy Sector Roadmap • Chemical Cyber Security • Guidance for Addressing Cyber Security in the Chemical Industry • Water Sector Roadmap	 DOE/SCC ACC/SCC ACC/SCC DHS/SCC	 2006 2006 2006 2008	 Plan Strategy Advisory Plan	Roadmaps provide detailed assessment of where the sector currently stands on initiatives for cybersecurity of control systems, and a plan for reaching an end state that provides for prevention, detection, and mitigation of attacks on these systems.
NSPD-54/HSPD-23	Presidential Directive	2008	Policy	Mandatory intrusion detection requirements for federal facilities.

2.2 Scope of the Strategy

The *Strategy* considers ongoing activities associated with the evaluation and mitigation of vulnerabilities and reducing the risk of control systems across critical infrastructures including:

- Coordinating mechanisms that include networking (individuals/organizations), the NIPP sector framework and public-private coordination and collaboration within that framework under the auspices of the CIPAC, and infrastructure protection processes and mechanisms developed within the NIPP sector framework
- Critical functional areas, including planning, research and development (R&D), recommended practices, incident response, information sharing, standards, and regulation
- Federal, state, and private sector programs and efforts

- Implementation goals and activities that can enhance coordination across government and private sector efforts.

The implementation of the *Strategy* will improve the overall coordination of control systems security initiatives by engaging stakeholders across all sectors.

2.3 Methodology

The implementation goals and activities in this document integrate information, recommendations, and approaches from two concurrent efforts: stakeholder engagement and document review.

2.3.1 Stakeholder Engagement

Stakeholders were identified as a critical resource to achieve a strategy with credibility and standing and for DHS to implement effective change. Stakeholders from recognized organizations within the NIPP sector partnership operating as public-private partners in critical infrastructure protection efforts under the auspices of CIPAC were identified to support the development and review of the document as it progressed. NCSD is pursuing the *Strategy* within the NIPP partnership framework, leveraging the CIPAC to enable public-private coordination and collaboration as the CSCSWG. Control Systems Federal Partner Working Group provides additional input and review to the *Strategy* effort.

Specific engagement activities consist of:

- DHS provides the vision and the planning for current and future coordinating activities across stakeholders in government and private sector.
- Operating and recognized by DHS as the NIPP partnership framework's private sector cross-sector council, PCIS engages the SCCs, CSCSWG addresses cross sector cyber risk and interdependencies. The CSCSWG serves as a forum to bring government and the private sector together to address common cybersecurity elements across all CIKR. PCIS also addresses cross-sector issues and interdependencies by providing a forum for to share important cross-sector issues.
- CSCSWG provides a cybersecurity focus and ensures coordination guidance is consistent with the NIPP partnership framework by providing a venue operating under the auspices of CIPAC to solicit information and obtain feedback on cybersecurity relevant to critical infrastructure protection.
- The Control Systems Federal Partners Working Group consists of government organizations that sponsored or participated in control systems security activities.

These activities include directed conference calls, formal and informal briefings to other public-private partnership entities within the NIPP partnership framework, working meetings with NIPP sector partnership members, workshops, internal and external review of control systems security products, and sharing of public products.

2.3.2 Document Review

Figure 2-1 illustrates the array of policy, strategy, and planning concepts incorporated from the current plans and efforts to secure control systems from cyber attack. These documents currently guide DHS' coordinating efforts to secure control systems from cyber attack.

The review of these documents provided a baseline for a "coordination landscape" and existing base of activities that need to be considered within the *Strategy*.

Figure 2-1. Inputs of existing stakeholder efforts.

This page intentionally left blank

3. STRATEGY

Control systems are an essential part of the nation's critical infrastructure and, as designed and operated, have the potential risk for unacceptable consequences from multiple hazards including a deliberate attack. As part of Sector Specific Plans (SSPs) for implementation, participants in public and private sector security partnerships are increasingly engaging in control systems security programs and protection efforts. The increased growth in effort corresponds to a rising awareness of system vulnerabilities and their potential to be exploited. Government agencies and private sector organizations aim to address the risk with technology development/deployment, situational awareness and threat analysis, development of security standards, information sharing, and incident response. The NIPP and other national strategy documents define the requirements, roles, and responsibilities for coordinating these efforts. NCSD serves as the lead agency for cybersecurity to the CIKR and provides coordination within the NIPP risk management framework supported by the NIPP sector partnerships framework. The *Strategy* will operate within that NIPP partnership framework, implemented to lead and engage security partners to a common vision.

3.1 Vision for National Coordination

The *Strategy* intends to provide guidance to aid in increasing and improving coordination on control systems security across all sectors. By utilizing the risk management framework and sector partnership model outlined in the NIPP, stakeholders can examine existing mechanisms for coordination and identify new opportunities for coordination. The *Strategy* will assist stakeholders in achieving a common vision of managing risk through the effective coordination of their activities.

Control systems security activities for critical infrastructures/key resources will be successfully coordinated across all sectors to effectively manage risk.

3.2 Guidance for Protecting Control Systems

The National Framework for Homeland Security, shown in Figure 3-1, illustrates the many sources of guidance, including legislation and strategy documents that will help stakeholders achieve this goal and that have guided the creation of this coordinating *Strategy*. There are existing efforts to secure control systems with associated mechanisms to establish goals and measure progress. Implementation of the *Strategy* is directed towards the building of opportunities that can lead to common goals, measures, and processes that demonstrate cybersecurity risk reduction in control systems.

3.2.1 Existing Mechanisms

The NIPP partnership framework, which organizes industry and government within relevant SCCs and GCCs and encourages their members to communicate and coordinate under the auspices of CIPAC, provides the capability to work with CIKR owners and operators to affect and support changes to improve the security of control system infrastructures. As these partnerships mature, government and the private sector are defining goals and metrics to an increasing level of detail. Several key mechanisms for setting goals and evaluating progress are described in this section.

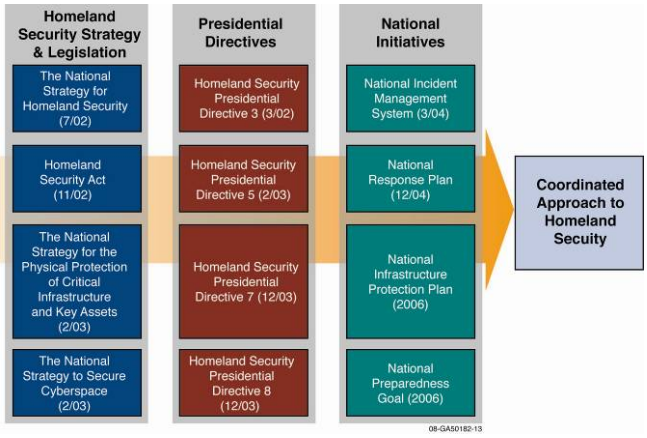


Figure 3-1. National Framework for Homeland Security (Figure 5.1 in NIPP).

3.2.1.1 Sector Specific Plans

HSPD-7 charged each SSA, in coordination with their SCC, with creating a SSP to address the requirements of the NIPP and develop the plan for

each sector's response to the risk management framework and to define coordination within the NIPP partnership framework. In several sectors, the SSPs identify control systems as an integral part of their cybersecurity critical infrastructure. Security goals identified by SSPs vary and apply to the needs of each sector. Though SSPs often cannot devote ample space to setting control systems security-specific goals and objectives, many sectors are recognizing the need for more detailed planning documents to address cyber and control systems security, such as sector strategies or roadmaps.

Across the sectors, there will be common control systems security issues, technologies, and opportunities for common solutions. The implementation of control systems security through the SSPs and derivative plans should identify and leverage these common elements.

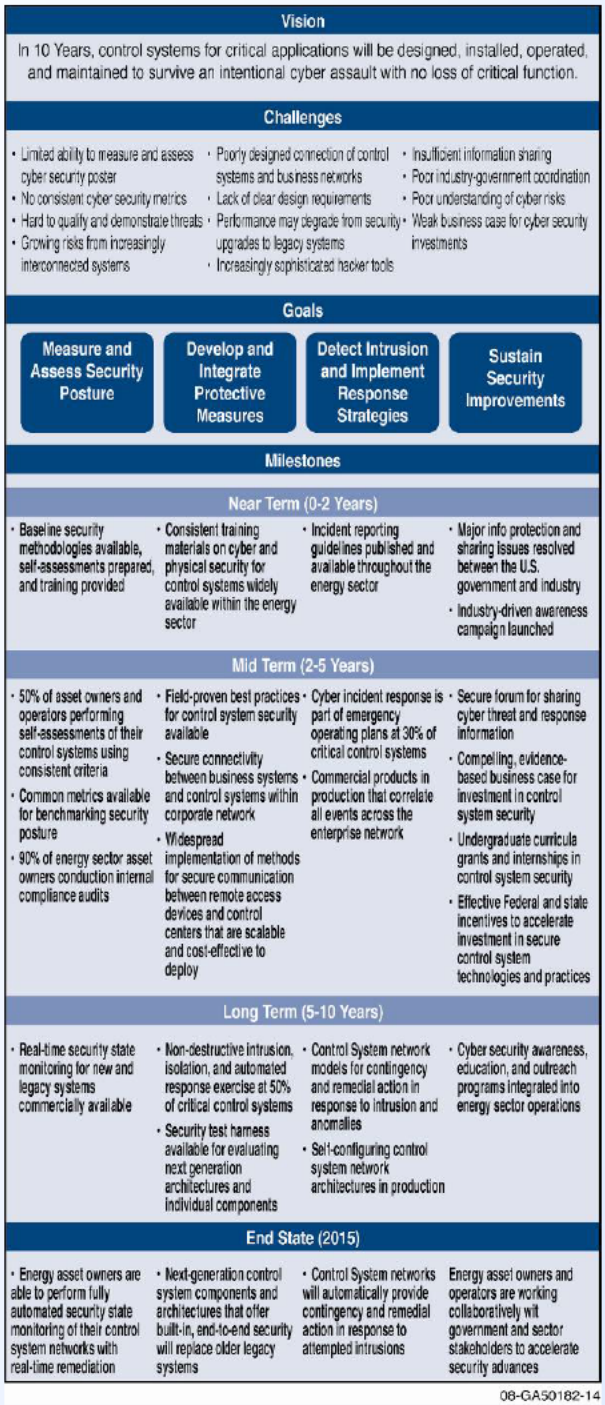
3.2.1.2 Sector Roadmaps

Several sectors are developing roadmaps that establish a vision for securing control systems within the sector, and include goals, objectives, measures, and timetables to meet the vision. Roadmaps develop a near, mid, and long-term perspective to guide industry efforts toward a common goal. Those created so far are detailed enough to enable stakeholders to evaluate their security posture, identify and resolve gaps in protective measures, and provide a consistent approach for reducing risks so that stakeholders can implement the high-level goals identified in the SSPs.

The Energy and Water Sectors have developed roadmaps that have had positive industry response. Other sectors are considering this approach. The Chemical Sector is currently developing a roadmap for securing control systems. The ACC published the *Chemical Sector Cyber Security Strategy*[4] in 2006 which alongside the Energy Sector and Water Sector roadmaps has provided a solid basis for developing the Chemical Sector roadmap.

These existing roadmaps will provide a template and starting point as other sectors begin to develop roadmaps to address the goals and objectives specific to their control system security needs.

DOE and the DHS sponsored the first roadmap, "A Roadmap to Secure Control Systems in the Energy Sector," which was released in January 2006. Predating the release of the NIPP, the roadmap provides actionable and measurable goals to achieve a higher level of control systems security.



4. *United States Chemical Sector Cyber Security Strategy*, "Chemical Sector Releases Updated Cyber Security Strategy," *Business Wire.* Sept 27, 2006. FindArticles.com. June 27, 2008, http://www findarticles.com/p/articles/mi_m0EIN/is_2006_Sept_27/ai_n16837022.

3.2.1.3 NIAC Recommendations

In a January 16, 2007 report to the U.S. President, the National Infrastructure Advisor Council (NIAC) recommended that the President "establish a goal, for all critical infrastructure sectors that no later than 2015, that control systems for critical applications will be designed, installed, operated, and maintained to survive an intentional cyber assault with no loss of critical function."[5] NIAC recognized that cyber attacks on critical infrastructure control systems can impact physical assets. The NIAC's subsequent analysis provides specific goals and recommendations for federal programs and the public-private sector partnerships to consider as they formulate plans to secure their control systems.

To guide sectors in developing sector-specific roadmaps, the NIAC made two recommendations:

1. The President should establish a goal for all critical infrastructure sectors that no later than 2015, control systems for critical applications will be designed, installed, operated and maintained to survive an intentional cyber assault with no loss of critical function (included as vision statement and timeline for the Energy Sector Roadmap).
2. DHS and SSAs should collaborate with their respective owner/operator sector partners to develop sector-specific roadmaps using the Energy Sector Roadmap as a model. (Water Sector Coordinating Council Cyber Security Working Group, "Roadmap to Secure Control Systems in the Water Sector," March 2008)

The complete description of the recommendations is provided in the referenced NIAC study. These recommendations are significant in that many are being incorporated into other stakeholder programs as goals and into the developing sector specific roadmaps. They are specific, broad reaching, and apply to both government and private sector stakeholders.

3.2.1.4 Federal Control Systems Security Programs

Several federal agencies also have programs that are focused primarily on control systems security. Goals and objectives for these programs are evolving, but are generally oriented toward short-term, value-added deliverables for their agency or the stakeholder community. They are also illustrative of the opportunities to coordinate, particularly within the federal sector.

Summaries of several of these programs are provided in Section 4. All Sector Specific Agencies have stakeholder interest in control systems security and in efforts to secure CIKR.

3.2.2 Implementation Goals

The goals of this strategy focus on agency or sector-specific efforts that generally have short term and incremental products and measures. The primary goal of the *Strategy* is to build a long-term common vision for control systems security and support actions on the part of the stakeholders. Recognizing that each stakeholder has their own priorities, resources, drivers, and constraints, a common vision also allows for common metrics, solutions, and tools that reduce uncertainty and risk for CIKR.

The implementation goals and detailed activities for the *Strategy* are provided in Section 5. These activities create an environment that can lead to the creation of a common vision to manage control system security risk across CIKR.

Summary of Implementation Goals

- Provide leadership in development of control systems security principles
- Assume full engagement in the NIPP partnership for control systems security
- Maintain a high level of outreach and awareness within the CIKR stakeholder community
- Advance performance measurement and feedback for control systems cybersecurity improvements in CIKR
- Coordinate and participate in the identification and analysis of gaps in control systems security technologies, policies, and planning
- Increase CIKR control systems security participation and role in incident response/information sharing

5. The NIAC Convergence of Physical and Cyber Technologies and Related Security Management Challenges Working Group, "Final Report and Recommendations by the Council," http://www.dhs.gov/xlibrary/assets/niac/niac_physicalcyberreport-011607.pdf, p. 3.

3.3 Coordination Framework

The NIPP provides a key element of the coordination framework. The integrated risk management framework shown in Figure 3-2 and the security partnership model shown in Figure 3-3 comprise the foundation for coordination across the CIKR. The risk management framework is the driver for setting security goals, identifying assets and functions, assessing risk, prioritizing efforts, implementing protections, and measuring effectiveness. It also drives key requirements (the what, why, how, and amount needed) for stakeholders to consider when evaluating protection of CIKR. This framework is recognized in SSPs and sector roadmaps.

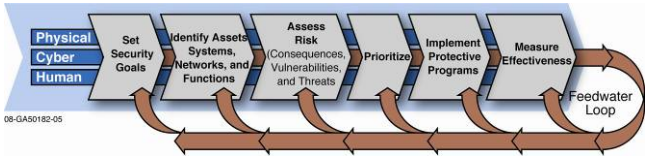


Figure 3-2. NIPP risk management framework.

Control systems security risk is derived from the threat potential for attack, vulnerabilities of systems to these threats, consequences of a successful attack, and mitigation of the vulnerabilities or consequences. A discussion of control system risks is in Appendix B.

3.3.1 Elements of the Framework

Figure 3-4 illustrates the correlation between the NIPP strategic framework as NIPP risk management/ security partnership model, coordination model, and implementation process. Integrating these three components is essential for a successful *Strategy*.

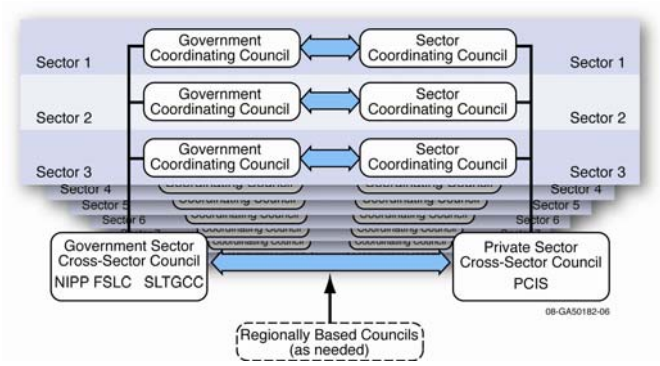


Figure 3-3. Sector partnership model.

3.3.1.1 NIPP Risk Management/Security Partnership Model

The NIPP partnership framework provides the partnership model for coordination and information sharing across public and private stakeholder groups. The framework defines what stakeholders need to do to protect CIKR and how those needs and outcomes will be measured and shared among stakeholders.

3.3.1.2 Proposed Coordination Model

Coordination within the integrated strategy framework occurs at programmatic, organizational, and functional levels, and is consistent with the respective roles and responsibilities defined in the NIPP. Separating coordination elements will provide insight into the opportunities that drive collaboration, avoid duplication of efforts, and identify gaps in security and protective measures.

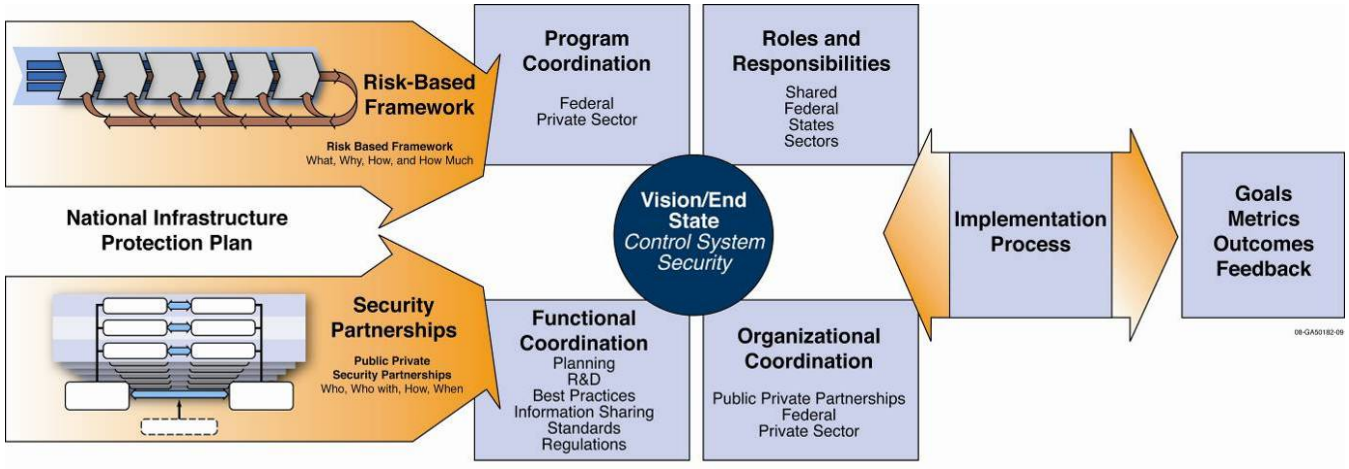


Figure 3-4. Framework for a coordinating strategy to secure control systems.

The coordination model presented in Figure 3-4 comprises the following four components that have a direct impact on the end-state of control systems security and, thus, the national coordination goals:

- *Roles and Responsibilities*. Overall guidance for government and private sector roles and responsibilities are provided by the NIPP and national strategy and policy directives. These roles and responsibilities provide the structure for security partnerships and pathways to define and implement coordination among stakeholders.
- *Program Coordination*. Public and private sector programs and initiatives focus on specific targets and opportunities needed to improve control systems security within a sector or across multiple sectors. Each program will have defined goals, products, metrics, investments, and schedules to achieve objectives. Programs may have overlapping stakeholders, sponsoring agencies or organizations, and applied technology or research.
- *Functional Coordination*. Functional areas include R&D, incident response, standards development, recommended practices development, training, regulatory guidance, and information sharing. These functional areas may share common goals, metrics, and products, but have different coordination mechanisms within the security partnership. For example, DOE and DHS both have research programs focused on control systems security. These agencies utilize several mechanisms to coordinate these programs.
- *Organizational Coordination*. Organizations that are stakeholders in control systems security have internal and external mechanisms for coordination. As an illustration, SSAs have significant responsibilities to coordinate activities within their sector, as well as within their internal divisions, related to research, regulations, and implementation of sector initiatives. The Office of Cybersecurity and Communication (CS&C), as the SSA for the Information Technology and Telecommunication sector, however, has a lead role in awareness and coordination with organizations spanning all agencies and sectors.

3.3.1.3 Implementation Process

The Implementation Process is the process of applying and enhancing the coordination mechanisms across public and private partnerships such as the Federal Partners, GCCs, and SCCs and their cross-sector councils and working groups. These groups address the requirements, measures, progress, and process of NIPP implementation by providing forums for discussion, planning, evaluation, and feedback.

The role of the implementation process, as illustrated in the coordination model, is to affect the coordinating mechanisms and resulting outcomes through the *Strategy*. The implementation of the *Strategy* fills the gaps and enhances the existing processes such that NPPD, as the lead organization for cybersecurity, can assist stakeholders in achieving the common vision for control systems security.

3.4 Roles and Responsibilities

Roles and responsibilities for CIKR stakeholders provide the context for coordinating activities. Overlap of roles and responsibilities exist and are either opportunities or barriers to enhanced coordination. This implementation of the *Strategy* will seek to constructively utilize these overlaps where they exist to improve coordination. The following provides a discussion that is derived from national strategies, presidential directives and policies, and national plans.

3.4.1 A Shared Responsibility: The Roles of Sectors, States, and Federal Government

Securing control systems is a shared responsibility among stakeholders throughout the control system value chain. The control systems stakeholder community consists of members within sectors, states, and federal organizations as shown in Figure 3-5, each of which brings specialized skills and capabilities to the effort of improving control system security:

- **Sectors** consist of owners and operators. They bear the main responsibility for ensuring that control systems are secure, for making the appropriate investments, for reporting incidents and vulnerability threat information to the government, and for implementing protective practices and procedures. They also need to report cyber incident threat information to vendors, researchers, and customers.
- **States** consist of regulatory bodies and emergency responders, who provide coordination and leadership with local and federal organizations during a crisis or incident.

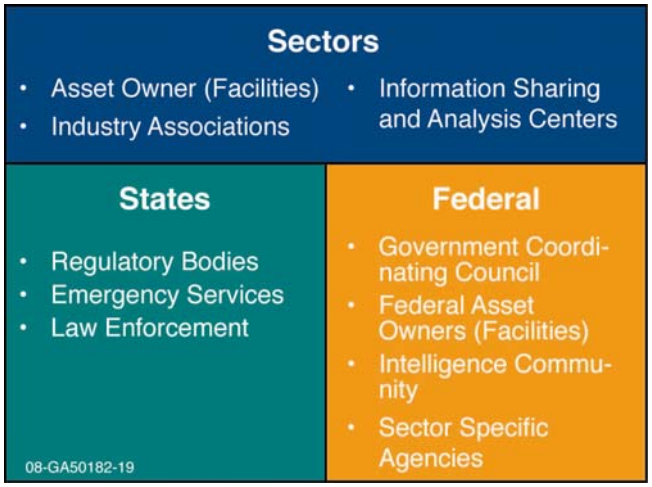


Figure 3-5. Key stakeholder groups share control systems security responsibilities.

- **Federal agencies** include the SSAs and Government Coordinating Councils that have responsibilities for control systems. The SSAs are also responsible to work with the Intelligence Community to provide emerging threat information and situational awareness briefings.

Seamless relationships among all participants that respond to the needs of the sectors, leverage resources effectively, and address cross-sector dependencies in an all-hazards context will accelerate the development and implementation of security solutions. Elaboration on stakeholder roles is found in the following sections.

3.4.2 Sector Characteristics and Commonalities

3.4.2.1 Owners and Operators

The NIPP defines the roles of private sector owners and operators of CIKR assets.[6] The owners and operators bear the main responsibility for securing and protecting assets in an environment that includes business interests, regulatory compliance and statues for operation, and a social responsibility their shareholders and the communities they serve.

The private sector invests in security based on operational risk and their competitive business environment. This is significant for control systems security because changes to physical control systems, software, policies, and procedures are more strongly influenced by productivity increases that provide economic benefits. Information channels for attack indications, warnings, and threat assessments are just becoming available to owners and operators. Private sector decision makers are also just becoming aware of the value of security investments.

The SSPs, along with their supporting roadmaps, provide recommendations to help owners and operators improve their security posture. The recommendations are relevant to existing and needed coordination mechanisms within the security partnership framework. Federal and private sector initiatives provide necessary resources to assist and leverage stakeholder efforts to implement the control systems security recommendations. The NIPP partnership framework provides the mechanisms for coordination and obtaining feedback.

Owners and operators are therefore encouraged to:

- Perform comprehensive risk assessments tailored to their specific sector, enterprise, or facility risk landscape
- Develop an awareness of critical dependencies and interdependencies at sector, enterprise, and facility levels
- Implement protective actions and programs to reduce identified vulnerabilities appropriate to the level of risk presented.
- Establish cybersecurity programs and associated awareness training within the organization
- Adhere to recognized industry recommended business practices and standards, including those with a cybersecurity nexus
- Develop and coordinate CIKR protective and emergency response actions, plans, and programs with appropriate federal, state, and local government authorities
- Participate in the NIPP partnership framework, including SCCs and information-sharing mechanisms, as appropriate
- Assist and support efforts to collect and protect federal, state, local, and tribal government data, as appropriate

6. Section 2.2.5, “Private Sector Owners and Operators,” National Infrastructure Protection Plan, Department of Homeland Security, 2006, p. 26–27.

- Participate in federal, state, local, and tribal government emergency management programs and coordinating structures
- Promote CIKR protection education, training, and awareness programs
- Establish resilient, robust, and redundant operational systems or capabilities associated with critical functions
- Adopt and implement effective workforce security assurance programs to mitigate potential insider threats
- Provide technical expertise to SSAs and DHS, when appropriate
- Participate in regular CIKR protection-focused exercise programs with other public and private sector security partners.

3.4.2.2 Vendors

The control systems vendor community is large and diverse. It provides technical services, hardware components and systems, application and operating system software, and integrated products. Many large control system vendors are internationally based, providing similar product lines for applications across sectors within the United States and abroad. Vendors rely on the competitive marketplace for their motivation to upgrade or advance features that enhance security. As an example, many legacy systems are not supported by the original vendor at all, but are maintained by the asset owner or contractor support.

Vendors generally respond to the needs of asset owners. Identified vulnerabilities and exploits to critical infrastructure control systems, whether affecting individual components or integrated systems, motivates asset owners to assert economic or contractual leverage to receive more secure systems from vendors. Asset owners should motivate vendors to upgrade control systems security in response to asset owner recommendations and security needs. The contractual responsibility of vendors to asset owners for security design and long-term support is a significant factor in defining their roles and responsibilities.

Control system vendors participate in groups that promote coordination across the private sector owner/operators and government organizations. The ICSJWG Vendor Subgroup, formerly known as the Control Systems Cyber Security Vendor Forum[7] is a mechanism used to address control system security issues and vendor response. Vendors also participate in standards organizations to work toward common requirements that provide additional assurance that security is being considered in the design and implementation of systems and functionality.

3.4.3 State, Local, and Tribal Governments

Each state has a significant role in the security of critical infrastructure located within its borders because of the potential impact failures can have on the safety and welfare of its citizens. Organizational frameworks may differ among states, but generally include a homeland security advisor, public safety and health organizations, and public utility commission that work with local and federal organizations during crises or incidents that fall within their constitutional or legislated roles and responsibilities. Municipalities that own and operate CIKR assets may have more significant coordination roles with these state and federal authorities. In some cases, states and local municipalities also own utility assets such as water, waste treatment, power, and communication networks, which extend their responsibilities to include the operation and maintenance of these systems.

3.4.3.1 Regulatory Bodies

State regulatory bodies exist to oversee the safety, environmental compliance, and taxation of industries within their purveyance. Control system security is also becoming an area of interest under the general category of cybersecurity. State executives and support organizations are thereby becoming more aware of control systems security issues and risks.

3.4.3.2 Emergency Responders

The control systems infrastructure resides primarily in the private sector, making cybersecurity the asset owner's and operator's responsibility. However, control system failure resulting from a cyber attack could have catastrophic and cascading consequences, placing heavy demands on state coordinated emergency response organizations.

7. NCSD Control Systems Security Program Web site: http://www.us-cert.gov/control_systems/index html.

According to the NIPP, federal grants are available in two broad categories to assist states in preparing to respond to cyber incidents[8]:
(1) overarching homeland security programs provide funding for a broad set of activities in support of homeland security mission areas and the national priorities outlined in the National Preparedness Goal, and (2) targeted infrastructure protection programs provide specific CIKR related protection initiatives and programs within identified jurisdictions. States should leverage all available resources, including federal, state, local, and tribal sources, as appropriate, to reduce vulnerabilities and close capability gaps related to CIKR within their jurisdictions. Each state is responsible to coordinate emergency response within its boundaries, which can involve federal, state, and local responders.

States' limited resources and expertise in control systems cybersecurity can be enhanced with requests to federal organizations with that expertise. The US-CERT provides incident information about cyber threats and vulnerabilities.[9] In addition, CSSP provides subject matter experts (SME) and analysis specific to control systems cybersecurity in response to US-CERT requests.

3.4.3.3 Information Sharing

Organizations such as the Information Sharing and Analysis Centers are providing resources and forums so organizations can better address their information technology (IT) and cybersecurity issues as well as other sector priorities. ISACs generally are aligned with a sector; however, state oriented organizations, such as the Multi-State ISAC (MS-ISAC), have membership from all 50 states and the District of Columbia. Representatives to MS-ISAC include many of the homeland security advisors and first responder organizations for the states.

3.4.4 Protective Security Advisors

DHS has placed highly experienced security advisors in the nation's major communities to assist with ongoing state and local critical infrastructure security efforts. The Protective Security Advisor (PSA) is a reach-back resource for DHS and other federal government resources and will:

- Support the development of the national risk picture by assisting in identification, assessment, monitoring, and minimizing risk to critical assets at the local or district level
- Facilitate, coordinate, and/or perform vulnerability assessments for local critical infrastructures and key resources
- Upon request, assist with security efforts coordinated by state Homeland Security Advisors

The PSA has training and awareness of the cybersecurity issues affecting critical infrastructure, including control systems, and have reach-back access to the DHS resources for support. The PSA also act as liaison between NIPP sector partnership entities, including SCCs and GCCs operating under the auspices of the CIPAC, and asset owners within their geographical region.

3.4.5 Federal Roles and Responsibilities

The NIPP and HSPD-7 direct the federal government to take the lead role in coordinating CIKR protection. HSPD-7 further directs DHS to provide overarching leadership in this effort. Each federal department and agency with programs that seek to improve control systems security serves a vital role in the broader federal effort to secure the nation's critical infrastructure control systems.

The federal government has the collective responsibility to address control systems security issues and provide end users (stakeholders) with information related to:

- Deterring threats:
  - Assess, analyze, and communicate threats/risks
  - Perform other intelligence and counterintelligence activities.
- Mitigating vulnerabilities:
  - Measure and assess security posture
  - Develop and deploy protective measures (new technology and R&D)

8. http://www.dhs.gov/xgovt/grants/.
9. http://www.uscert.gov.

- Share information and recommended practices (for legacy systems)
- Minimizing consequences:
  - Perform consequence analysis and cross-sector interdependencies
  - Detect and mitigate incidents
  - Respond, recover, and reconstitution.

3.4.5.1 DHS and CSSP

HSPD-7 designates the DHS as the federal agency responsible for leading, integrating, and coordinating the overall national effort to enhance CIKR protection. It also names DHS as the focal point for securing cyberspace for CIKR. The NIPP outlines many DHS roles and responsibilities; for example, "identifying, prioritizing, and coordinating federal action in support of the protection of nationally critical assets, systems, and networks…" and "…coordinating national efforts for the security of cyber infrastructure, including precursors and indicators of an attack, and understanding those threats in terms of CIKR vulnerabilities."

Reducing risk requires an integrated approach that encompasses both physical and virtual threats and their associated human elements. The Office of Cybersecurity and Communications (CS&C) has the mission of assuring the security, resiliency, and reliability of the nation's cyber and communications infrastructure. A division within CS&C is the NCSD, which works collaboratively with public, private and international entities to secure cyberspace and America's cyber assets. NCSD has two overarching objectives for protecting the cyber infrastructure: build and maintain an effective national cyberspace response system, and implement a cyber risk management program for critical infrastructure protection. CSSP is NCSD's focal point in accomplishing these goals for control systems.

CSSP is coordinating activities among federal, state, local, and tribal governments and control systems owners, operators, and vendors to reduce the risks of a cyber attack on control systems in CIKR sectors. Part of developing a strategy for federal efforts is understanding how existing federal control systems operate and coordinate—collectively fulfilling the federal role in infrastructure protection.

To address this challenge, NCSD organized the Federal Partners Working Group, which is made up of representatives from across the federal agencies who have controls systems security interests (read more about the Federal Partners in Section 3.5.2). The Federal Partners organized a data call to query federal agencies on their current control systems activities and how they collaborate with other organizations to achieve security objectives. The results of that data call and a framework for continued coordination throughout federal agencies was designed to contribute to the development of the *Strategy*.

3.4.5.2 Responsibilities of SSAs

The NIPP partnership framework designates SSAs as government representatives from each sector that, in accordance with HSPD-7, are responsible for collaborating with all relevant federal departments and agencies, state and local governments, and the private sector, including key persons and entities in their infrastructure sector; implementing their sector's SSP; conducting or facilitating vulnerability assessments of the sector; and encouraging risk management strategies to protect against and mitigate the effects of attacks against CIKR.

3.4.5.3 Mission and Intelligence Agencies

Many agencies conduct mission-related activities or maintain key capabilities and resources for improving control systems security. These activities include surveillance, technology research, regulation, and support for control system operation and related commerce. For example, the National Institute of Standards and Technology (NIST) works to develop industry standards; the Central Intelligence Agency (CIA), Federal Bureau of Investigations (FBI), and DOD develop threat intelligence; and the Federal Energy Regulatory Commission (FERC) and Nuclear Regulatory Commission provide regulatory oversight.

3.4.5.4 Federal Owners and Operators

Some federal agencies own and operate control systems as part of their facilities and operations. Much like owners and operators in the private sector, they are responsible for implementing prudent protective measures and making appropriate investments to improve security. Examples of federal owners and operators include DOD, which supports the military industrial complex, and the Department of the Interior's Bureau of Reclamation, which manages water resources in the western United States.

3.4.5.5 Regulatory Bodies

The federal government has regulatory authority over several areas of the CIKR that have specific interest in control systems security. The interest and focus has increased due to the potential consequences of a catastrophic failure or successful exploit of vulnerabilities of these systems. Several significant regulatory bodies with roles and responsibilities that include control systems security are:

- The Nuclear Regulatory Commission has the oversight and regulatory responsibility for commercial nuclear power plants' design and operations including physical and cybersecurity.
- The Environmental Protection Agency has the mission to protect human health and the environment. Since 1970, EPA has been working for a cleaner, healthier environment for the American people.
- The FERC has oversight and regulates the interstate transmission of electricity, natural gas, and oil. This commission works with the North American Electric Reliability Corporation (NERC) to administer standards for compliance to the energy sector's critical infrastructure.
- The DHS was granted authority in 2006 to provide regulatory authority over chemical facilities considered high risk to terrorist attack. This oversight includes the physical and cybersecurity of these facilities.

3.5 Existing Coordinating Mechanisms

A key step in developing a comprehensive coordinating strategy is to create a baseline from the current coordinating mechanisms. The Federal Partners identified 33 coordinating mechanisms during a workshop held March 5, 2008.

This section provides an overview of the control systems coordinating mechanisms that currently exist through the public-private security partnerships developed within the NIPP partnership framework and leveraging the CIPAC to collaborate and coordinate on critical infrastructure protection issues, NIPP processes and mechanisms developed by the sectors, and other industry and government coordinating conduits. Each of these areas is presented in Table 3.1. The table illustrates functional coordinating mechanisms organized by networks, partnerships, and processes:

- **Organizations** enhance control systems security situational awareness and maximize exchange of information between government and private sector security partners at all levels. Networks also help assess risks and execute risk-mitigation programs and activities.
- **NIPP sector framework and public-private groups operating under the auspices of CIPAC** are NIPP public, private, or joint public-private entities formed through the sector partnership model. Members of these groups represent public and/or private partners engaged in joint control systems protection-related activities.
- **NIPP Processes and Mechanisms** ensure that effective policies, approaches, guidelines, and methodologies regarding control systems partner coordination are developed and disseminated to enable SSAs and other security partners to carry out NIPP responsibilities.

The purpose and description of these coordinating mechanisms are detailed in Appendix C.

The remainder of this section describes the main public-private, federal, and private sector coordination efforts and the key activities they pursue, planning, R&D, recommended practices, incident response, information sharing, standards, and regulation.

3.5.1 Public-Private Coordination through NIPP Sector Partnership Processes Enabled by CIPAC

Addressing the complex and dynamic challenges in control systems security typically requires partnerships among diverse organizations in the public and private sectors. Many federal activities provide support and solutions for the owners and operators of control systems, who are primarily in the private sector. Public-private partnerships have proven effective in ensuring that these solutions are viable in commercial operations. Similarly, researchers from the public and private sector are working together to advance science and technology research. As examples, commercial firms that sell, install, and service control systems and enabling resources are participating in federal research, assessment, and training programs. International partners are also contributing to efforts to improve security standards.

Table 3-1. Public – Private Coordinating Mechanisms in Control Systems Security.

Functional Areas	Coordinating Mechanisms: Organizations (see Appendix C)																						NIPP Sector Partnership & NIPP Public-Private Groups					NIPP Processes & Mechanisms			
	CERT-CC	FBI InfraGard	Federal Partners Working Group	Fed Plan CS IA R&D	GFIRST	HITRAC	ISACs	ISA	ieRoadmap	IEC	Joint Terrorism Task Force	Law Enforcement Online	MS-ISAC	NCRCG	National Exercises-Cyber Storm	NICC	NIPP Protection Metrics WG	ODNI	PCSRF	Standard Authorization Request	TSWG	US-CERT	Cross Sector Cyber Security WG	Energy Sector Control Sys WG	ICSJWG	PCSF	WSCC Cyber Security WG	HSIN	SAR/NAR	NIPP Sector-Specific Plan	National R&D Plan
Research and Development				■	■	■			■												■			■			■				■
Assessments and Analyses	■			■	■	■			■		■							■			■	■		■			■	■			
Training		■			■			■			■				■												■				
Recommended Practices		■		■	■		■			■	■		■	■	■		■		■		■		■	■	■	■	■			■	■
Outreach, Awareness, and Information Sharing	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■
Standards Development				■		■	■	■		■	■		■						■	■							■				
Policy/Regulation Coord. and Development														■			■		■				■	■	■	■	■		■	■	
Law Enforcement						■					■	■		■			■														
Acquisition and Procurement							■																								
Partnership Development		■	■	■		■	■	■	■		■	■	■		■		■						■	■	■	■	■	■		■	■
Vulnerabilities Disclosure	■	■		■	■	■	■		■			■	■	■		■	■					■		■			■				
Threat Information	■	■		■		■	■		■		■	■	■	■	■	■	■	■			■	■		■	■		■	■	■		
Metrics				■					■								■							■							
Interdependency Issues		■	■	■		■	■		■		■		■	■	■		■						■	■	■	■	■		■	■	
Business Continuity							■							■	■		■								■		■				
Incident Reporting and Situational Awareness	■	■			■	■	■		■		■	■	■	■	■	■	■				■	■			■		■	■			

The NIPP provides a sector partnership framework upon which public-private coordination and collaboration can build under the auspices of CIPAC. These public-private partnerships can improve infrastructure protection across all CIKR sectors. Through this framework, security partners are beginning to recognize and address similarities and differences between approaches to control systems risk management for business continuity and national security. Security partners should continue to use the NIPP partnership framework to work collaboratively, leveraging cyber-specific expertise and experience, and improving information exchange and awareness of control systems security concerns. These partnerships will enable public and private entities to make informed control systems risk management decisions, define national control systems priorities, and address control systems security as part of an overall national CIKR protection strategy.

3.5.2 Federal Coordination by Federal Partners Working Group

In January 2006 the Federal Partners formed to lead government coordination to secure critical infrastructure control systems. Created under the NCSD, Federal Partners joins leaders from more than 30 federal organizations together to promote coordination among federal agencies by voluntarily sharing information about control systems activities.

In late 2006, Federal Partners began an effort to develop an organizing framework for federal activities. This work included base lining information on existing federal coordination initiatives to improve the understanding of federal activities across agencies and increase opportunities for leveraging. To do so, Federal Partners developed an electronic data call to query federal agencies on their current activities in control systems, their program or agency objectives in performing those activities, and the mechanisms they use to coordinate with other agencies or organizations.

Federal Partners contacted 67 federal programs to complete the data call in April of 2007 and 2008. By May 2008, the Federal Partners received 31 responses from 28 organizations, including 12 SSAs. The Federal Partners incorporated the results into the *Federal Strategy*, which outlines the vision, roles, and framework for federal coordination efforts. The document describes the current coordination efforts by both the problems they attempt to address and the activities pursued to address those issues.

The efforts of Federal Partners have now been integrated into this coordination *Strategy*, which guides federal, state, and private sector initiatives across the critical infrastructures.

3.5.3 Private Sector Coordination

Despite the effectiveness of public-private partnerships and federal efforts, certain responsibilities necessarily remain strictly private. Private entities that own and operate control systems bear the primary responsibility for investing in and implementing the measures necessary to protect the critical functions of their systems. Many private sector organizations are active members of multiple working groups, which assist in providing planning, R&D, recommended practices, and incident response.

Threat and vulnerability and mitigation information must be shared in order to better protect all systems throughout the nation. To better facilitate coordination of private sector activities, all organizations are encouraged to participate in appropriate coordinating mechanisms described in the *Strategy* and that are most relevant to their specific needs. Active engagement in these mechanisms will maintain consistency and continue progress in building technology and partnerships.

Private sector coordinating mechanisms, such as Information Sharing and Analysis Centers, Partnership for Critical Infrastructure Security, SCCs, and the formal and informal professional, academic, and trade associations facilitate activities that make control systems more secure. Using and enhancing these mechanisms to securely share information will help continue building industry trust, which will increase information sharing, and enable private companies to better protect their assets.

3.5.4 Government and Private Sector Coordination

The ICSJWG provides the mechanism to coordinate government and private industry security initiatives. ICSJWG was established to continue the successful public and private partnerships started by the Process Control System Forum (PCSF).

The ICSJWG is a collaborative and coordinating body created within the NIPP partnership framework that enables public-private collaboration and coordination under the auspices of CIPAC. The ICSJWG provides a vehicle for communicating and

partnering across all CIKR between federal agencies and departments, as well as private asset owner/operators of industrial control systems. ICSJWG, as defined by its charter, facilitates the collaboration of the industrial control systems stakeholder community in securing CIKR by accelerating the design, development, and deployment of secure industrial control systems.

3.5.5 Planning

The NIPP and National Response Framework (NRF – see Section 3.5.7.5) require the development, coordination, and implementation of plans that target CIKR security improvements. Sector specific plans and roadmaps are being developed and will have a positive strategic impact on the security of control systems across the various sectors. The public-private partnership entities that develop these plans and the federal SSAs activities are the principal coordination mechanisms. The Energy and Water sectors have already developed roadmaps for their sectors and approved them through their respective Coordinating Councils. These planning activities allow CIKR stakeholders to focus on common issues and long-term planning that have sector or cross-sector impact, and which will compliment business or corporate specific goals.

3.5.6 Research and Development

R&D initiatives to improve CIKR security are performed by government, academic, and private sector organizations, therefore, coordination must occur at and across all these areas.

The *National Critical Infrastructure Protection Research and Development Plan* (NCIP R&D Plan), developed in partnership with DHS and the Office of Science and Technology Policy, provides themes and objectives for short- and long-term security improvements. The NCIP R&D Plan also highlights CIKR security accomplishments and activities of government agencies. In 2007, the DHS Science and Technology Directorate further described CIKR R&D coordination mechanisms, roles and responsibilities, and government research priorities in *Coordination of Homeland Security Science and Technology*.

To support R&D efforts outside the federal government, CSSP works with control systems vendors to provide avenues for organizations to share information and coordinate projects and results among themselves and with government sector specialists. As an example, NPPD coordinates with the DHS Directorate for Science and Technology (S&T) in support of the control systems security aspects of the consortium, Linking the Oil and Gas Industry to Improve Cyber Security and the Institute for Infrastructure Information Protection (I^3P).

3.5.7 Recommended Practices

The NIPP encourages the development and sharing of recommended practices to achieve secure CIKR. Industry and government are actively developing and promulgating recommended practices as a coordination mechanism to achieve common improvements in many areas. The SSPs also include recommended practices as a common goal, which is reflected in sector-specific roadmaps. Control systems security recommended practices are being supported by collaboration within DHS, NIST, DOE, industry groups, and state organizations. These practices are viewed as general guides that can be tailored to site and sector-specific applications.

Since the recommended practices are products of collaborative work by government and industry, they provide significant opportunities for coordinating efforts within and across sectors that have related stakeholders such as suppliers, system integrators, academia, and standards organizations. The website for NCSD US-CERT Control Systems (http://www.us-cert.gov/control_systems/) provides access to the recommended practices, standards, and guidance relevant to control systems cybersecurity. The ICS-CERT[10] provides analysis of current vulnerabilities and exposures that have potential for impacting control systems to US-CERT, which develops alerts and recommended mitigations strategies for public release.

10. The Control Systems Security Program operates the ICS-CERT and works with US-CERT to support the control systems risk reduction mission (http://www.dhs.gov/xgovt/grants/).

3.5.8 Incident Response

Incidents of national significance have spurred greater involvement by organizations, which have contributed to an overall response capability now being nationally coordinated through the National Response Framework. However, NCSD is primarily responsible for coordinating cyber emergency response and information requests for control systems cybersecurity incidents through the US-CERT.

3.5.8.1 US-CERT

Established in 2003, US-CERT is charged with providing situational awareness information (based on continuous evaluation) for the nation's Internet infrastructure by coordinating defense against and response to cyber attacks. The agency is responsible for analyzing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities. US-CERT disseminates consistent and actionable cybersecurity information to the public through interaction with federal agencies, industry, the research community, state and local governments, and others.

US-CERT interacts with government and private sector entities to coordinate functions and programs. It reports on vulnerabilities, performs follow-up analyses, and shares information to alert owners and operators. US-CERT's coordination efforts are guided by operational procedures.

NCSD has developed and operates the Einstein program in conjunction with US-CERT as a part of its role to protect government IT resources. This program is an automated process for collecting, correlating, analyzing, and sharing computer security information across the federal government to improve our nation's situational awareness.

3.5.8.2 Control Systems Security Program

The CSSP manages and operates the ICS-CERT in collaboration with the US-CERT for control systems related incidents and cybersecurity situational awareness activities. This provides the US-CERT SOC with control systems analysis capabilities including incident response, vulnerability analysis, and responding to general requests for information. A core component of the ICS-CERT is the Control Systems Security Center (CSSC). This component offers additional analysis capabilities, including testing and evaluating impacts of vulnerabilities and malware on realistic control system configurations.

3.5.8.3 National Infrastructure Coordinating Center

The Department of Homeland Security's National Infrastructure Coordinating Center (NICC) serves as a focal point for coordinated CIKR incident-related information sharing with the owners/operators of the nation's CIKR and federal SSAs.

Functional coordination for control system related incidents or requests for information occur through the US-CERT to the CSSP.

3.5.8.4 National Operations Center

Information is shared and fused on a daily basis by the two halves of the DHS Office of Operations Coordination: the "Intelligence Side" and the "Law Enforcement Side." The two pieces fused together create a real-time snap shot of the nation's threat environment at any moment. Through the National Operations Center, the Office provides real-time situational awareness and monitoring, coordinates incidents and response activities, and, in conjunction with the Office of Intelligence and Analysis, issues advisories and bulletins concerning threats to homeland security. The National Operations Center operates 24 hours a day, seven days a week, 365 days a year, to coordinate information sharing that will help deter, detect, and prevent terrorist acts and to manage domestic incidents. Information on domestic incident management is shared with Emergency Operations Centers at all levels through the Homeland Security Information Network (HSIN).

Functional coordination with respect to control systems-related incidents or requests for information occurs through the US-CERT to the CSSP.

3.5.8.5 National Response Framework

The NRF (http://www.fema.gov/emergency/nrf/) presents the guiding principles that enable all response partners to prepare for and provide a unified national response to disasters and emergencies—from the smallest incident to the largest catastrophe. The NRF establishes a comprehensive, national, all-hazards approach to domestic incident response. Although it replaces the National Response Plan, the NRF's incident annexes are still in effect.

3.5.8.6 DHS-NCSD Role in the Cyber Incident Annex

The NCSD plays a supporting role in the event of a cyber attack on critical infrastructure. The functional coordination of incident response and requests for information during a cyber attack of a control system would occur through the US-CERT to the CSSP.

3.5.8.7 National Cyber Response Coordination Group

The National Cyber Response Coordination Group (NCRCG) is comprised of senior representatives from federal agencies that have roles and responsibilities related to preventing, investigating, defending against, responding to, mitigating, and assisting in the recovery from cyber incidents and attacks. In the event of a major cyber-related Incident, requiring federal response and interagency coordination, the NCRCG is convened to harmonize operational efforts and facilitate information sharing.

For incidents or information requests regarding control systems security, functional and organizational coordination occurs through NCSD participation in the NCRCG. SMEs in control systems cybersecurity are provided on an as needed basis and when requested from NCRCG.

3.5.8.8 Cyber Exercises

NCSD designs and coordinates exercises such as the "Cyber Storm" series. These exercises generally include control systems incidents scenarios involving multiple federal, state, local, and private sector stakeholders.

In support of this mission, the CSSP provides subject matter expertise in the development and planning of critical infrastructure scenarios that include control systems.

3.5.8.9 Government First Incident Response Security Teams

The Government First Incident Response Security Teams (GFIRST) is a group of technical and tactical practitioners from security response teams responsible for securing government IT systems. GFIRST members work together to understand and handle computer security incidents and to encourage proactive and preventive security practices across government agencies. Participants represent local, state, and federal agencies. Coordination occurs through training, conferences, and information sharing and distribution through a secure portal sponsored by US-CERT.

NCSD, sponsor of GFIRST activities, coordinates control systems security, which includes training, technical briefs, and demonstrations from control systems security SMEs.

3.5.9 Information Sharing

The public-private sector partnership framework of the NIPP establishes the basis for information sharing. Owners and operators of CIKR need information on risks and hazards to affect decisions and guide investments to protect their infrastructure. The government needs information from the private sector to adjust their programs that support protection activities. Sharing of control systems security information generated by federal programs or interactions with other public and private sector organizations is thus an important element of risk reduction. Information to be shared includes situational awareness, threats, vulnerability detection and mitigation, training, recommended operating and assessment practices, security standards, and performance metrics.

Many coordinating mechanisms facilitate control systems security information sharing within government, cross-sector, and sector-specific organizations. Agencies that have demonstrated specific roles in sharing control systems security information are described in Table 3-2.

The CSSP, through formal and informal relationships with asset owner/operators and control systems vendors, provides a means for coordinating incidents and disseminating vulnerability or alert information through the ICS-CERT.

3.5.9.1 Information Sharing and Analysis Centers

The ISACs provide a focus for private sector collection, analysis, and distribution of critical infrastructure data for the functional or sector specific group of stakeholders. US-CERT also provides a coordination function for receipt and analysis of information from the private sector for use by the government in managing cybersecurity incidents. It is *important* to note that not all sectors have ISACs.

Table 3-2. Demonstrated specific roles in the sharing of control systems security information.

Government Sponsored Programs	
US-CERT	Provides pubic and secure-facing Web sites with information and analysis on vulnerabilities and incidents. Hosts a Control Systems secure site for information sharing to a variety of stakeholders.
Federally sponsored programs	Fund control systems security specific products and demonstrations that are distributed to stakeholders including incident reporting, situational awareness, technology, training, and outreach through conferences, Web sites, and working groups. • DHS CSSP • DHS Science and Technology Critical Infrastructure Protection focus area • DOE National Supervisory Control and Data Acquisition (SCADA) Test Bed.
Control Systems Federal Partners Group hosted by NCSD	Provides a forum to periodically discuss issues affecting government programs involved in control systems security and critical infrastructure. Also provides a mechanism for various government agencies to coordinate cyber security across the sectors in areas of their responsibility.
Sector-Specific Agency Executive Management Office (SSA EMO)	The SSA EMO, an office within the DHS Office of Infrastructure Protection, serves as the SSA for six of the 18 CIKR Sectors. These include Chemical, Commercial Facilities, Critical Manufacturing, Dams, Emergency Services, and the Nuclear Sectors. SSA EMO programs cover the physical, human, and cyber aspects of security. The SSA EMO coordinates with sectors and on NCSD control systems risk reduction efforts.
HITRAC	The Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), coordinating with the Intelligence Community and other government agencies, provides threat briefings to government and private sector entities to include control systems security content when incidents or situational awareness may indicate a need.
HSIN	The Homeland Security Information Network (HSIN) provides participants with secure information-sharing capability with government and within private sector.
NICC	The National Infrastructure Coordinating Council provides a mechanism for the private sector to seek information regarding control systems security relevant to their sector.
InfraGard[a]	InfraGard is a partnership between the FBI and the private sector. InfraGard is an information-sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members including businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. InfraGard provides an outlet for government and private sector information on control systems security issues including forensic analysis, vulnerabilities, and threat information.
CIPAC	The Critical Infrastructure Partnership Advisory Council is a key enabler developed to support critical infrastructure protection associated with the NIPP partnership framework. The CIPAC enables coordination and collaboration between government and CIKR owners and operators on critical infrastructure protection issues, providing a forum in which they can together engage in a broad range of communication, coordination, and collaboration across the critical infrastructure protection risk management spectrum.
ICSJWG	The Industrial Control System Joint Working Group consists of government and private sectors stakeholders specifically focused on control systems security issues which provided the forum for a number of industry focus subgroups. These subgroups focus on current security issues and develop goals and supporting tasks to address these issues. Information sharing will also be facilitated via teleconferences, working group meetings, technical papers, and via the CSSP Web site.
Public–Private Sector Partnerships	
The ICSJWG Control Systems Security Vendor Subgroup	An ICSJWG subgroup of subject matter experts who represent the control systems vendors. Information sharing includes teleconferences focusing on common security areas of interest. Facilitated by the CSSP, the group shares common concerns, questions regarding government programs and products, and a vendor perspective of security needs. The vendors participating represent the majority of control systems installed base globally, not just the United States.
ISACs	Information Sharing and Analysis Centers provide a framework for sector or technology collecting, vetting, and sharing information relevant to its member stakeholders. There are currently 11 ISACs with an ISAC council.[b] ISACs with specific activity in control systems security have included the Multi-state ISAC[c] and the electrical ISAC[d] sponsored by the North American Electrical Reliability Corporation.

a. http://www.infragard.net/
b. http://www.isaccouncil.org/about/
d. http://www.msisac.org/
e. http://www.esisac.com/

In the cases where sector ISAC's do not exist, the sectors rely on their SSA to perform the information-sharing function.

The functional coordination of incident response and requests for information for a cyber attack of a control system would occur through the US-CERT to the CSSP.

3.5.10 Standards Bodies

Standards bodies provide significant opportunities for cross sector stakeholder coordination. The process for developing standards provides a forum for stakeholders (asset owners, operators, vendors, and regulators) to advance technical and administrative recommended practices that address evolving security needs. Standards organizations such as the Instrumentation, Systems, and Automation Society (ISA), Institute for Electrical and Electronics Engineers, the International Electrotechnical Commission (IEC), and NIST provide standards related to control systems security. Individual sectors industry organizations, such as the American Gas Association and NERC, are also developing standards where gaps exist in technology for securing control systems.

Government-Private Sector partnerships have developed several products that support information sharing and functional coordination during standards development:

- *Catalog of Control Systems Security*. Recommendations for Standards Developers: This catalog presents a compilation of practices that various industry bodies have recommended to increase the security of control systems from both physical and cyber attacks. The recommendations in this catalog are grouped into 18 families (categories) that have similar emphasis and can be used by all sectors to develop a framework needed to produce a sound cybersecurity program.
- *Cyber Security Procurement Language for Control System*. This catalog presents a compilation of practices that various industry bodies have recommended to increase the security of control systems from both physical and cyber attacks. The catalog is general enough to provide guidance across all sectors.

The NCSD is providing functional coordination with these standard bodies and subject matter expertise support. NCSD is working to develop and execute a strategy for the DHS involvement and prioritization of control systems security on multiple standards activities.

3.5.11 Benchmarking Tools

NCSD recognizes the importance of developing a means to measure the degree to which cybersecurity is being implemented within the ICS environments. To assist asset owners NCSD has developed the following tools:

- *Control Systems Cyber Security Self Assessment Tool (CS2SAT).* The CS2SAT is a desktop software tool that guides users through a step-by-step process to collect facility-specific control system information and makes recommendations for improving the system's cybersecurity posture. The source of requirements utilized in the tool is industry standards and guides relevant to control system security compliance and recommended practices. The tool can be customized to specific industries.
- *Cyber Security Vulnerability Assessment Tool (CSVA).* The CSVA is an assessment tool similar to the CS2SAT with a primary focus on IT systems. Developed to support sector Comprehensive Reviews for IT assessments, it is applicable to those components common to both control systems and IT systems.

In addition, many SSAs have implemented programs to facilitate awareness of the benchmarking tools described above. For example, the Chemical Sector has implemented the Security Outreach and Awareness Program (SOAP) in order to bring the CSVA to small and medium sized facilities.

NCSD will continue to support outreach and awareness activities for benchmarking tools and develop additional risk mitigation measures to support the asset owner's cybersecurity mission.

3.5.12 Regulation

The regulatory environment for critical infrastructure includes federal, state, and local entities that have traditionally governed safety and environmental compliance. For example, federal regulation of electric power transmission at locally owned power generation and distribution facilities is governed through FERC and NERC. The Environmental Protection Agency oversees water, waste treatment, and other sources of industrial

pollution. DHS has been given regulatory authority over the Chemical Sector because of the potential for terrorists to seriously impact the health and welfare of citizens using chemical facilities as weapons of mass destruction.

Regulations requiring specific cybersecurity standards or requirements for control systems are sparse. The NERC Critical Infrastructure Protection standards provide general guidelines for physical and some cyber protection of critical assets. For the Chemical Sector, the Office of Infrastructure Protection has provided regulatory guidance by the Chemical Facility Anti-Terrorism Standards (CFATS). Specific Risk Based Performance Standards (RBPS) have been developed that include control systems cybersecurity. These standards were written in coordination with NCSD and align with NCSD recommended programs and tools.

These SSAs routinely meet with CIKR stakeholders to address the implementation of and compliance with standards States and local public utility commissions' are responsible for engaging in the regulatory process as owner-operators, regulators, or CIKR stakeholders in the regulator process.

The Energy and Water Sectors have developed roadmaps for control system security that advances the implementation of the sector specific plans. The Chemical Sector is currently in the processes of developing a Roadmap to Secure Control Systems in the Sector. CIKR stakeholders view the roadmaps as a means to articulate cybersecurity requirements to a broad and diverse stakeholder community.

3.6 Performance Outcomes for Federal Agencies

SSAs collaborate with their security partners in industry, state and local governments, and the federal government to improve control systems security and reduce overall risks to critical assets and systems. Working through the NIPP partnership framework and the risk management framework, SSAs help encourage information sharing and analysis, develop protective programs, promote good security practices, and measure progress in reducing physical and cyber risks to the control systems and the assets they operate. In short, the SSA has a central role in understanding its sector's cybersecurity needs and working with its sector counterparts to coordinate control system security efforts.

The NIPP recognizes that every CIKR sector has unique characteristics, business models, and risk profiles that help define their infrastructure protection strategy. This is particularly true for control systems, which are used for a variety of purposes and at different scales across the CIKR sectors. Each SSA must work with its members to develop tailored approaches to managing risks for their specific assets. However, a common framework of recommended practices can be implemented by all SSAs to ensure a comprehensive approach to risk management.

3.6.1 Common Understanding of Sector Control Systems Needs

Each particular application of a control system network has distinct operating requirements, technical needs, and protection issues. There are however many common characteristics applicable across CIKR sectors. Each SSA should have a comprehensive understanding of the particular control systems security needs of the sector it works with. This may require the SSA to identify SMEs who can provide insights about the cyber aspects of their sector. SSAs and their SMEs should work with owners and operators to develop a common understanding of security needs that covers such areas as assessing risks, new technologies, vulnerability testing, detection and response, information sharing, training, and outreach. For example, owners and operators in the energy and water sectors have developed and published comprehensive roadmaps that identify their vision for securing control systems, major goals, key challenges, and prioritized needs to overcome those challenges. Some sectors have formed working groups to outline their major cybersecurity needs. The development of a roadmap, plan, or analysis of the cybersecurity needs for each sector builds a strong foundation for implementing actions and programs that can reduce both near and long-term risks.

3.6.2 Public-Private Partnership and Engagement

The NIPP, with the enabling support of CIPAC, provides a comprehensive framework for facilitating public-private partnerships to improve infrastructure protection in the CIKR sectors. Each SSA manages the overall process for building security partnerships and leveraging CIKR security expertise, relationships, and resources for its sector. SSAs should use the NIPP partnership framework to collaborate with

sector owners and operators on efforts to reduce risks to control systems

Partnership activities that focus on control systems security have been initiated in several of the sectors that have significant control systems assets. For example, several sectors, including Electric, Oil and Gas, and Water, have established cybersecurity working groups operating under the auspices of CIPAC to address cyber risks and implement control system projects and plans. DHS and the NIPP partnership framework's private sector cross-sector council (PCIS) also created the CSCSWG to bring together industry and government to share information and implement activities across all sectors. The CSCSWG provides a forum for public and private sector experts to collaborate on control systems security issues that affect multiple CIKR sectors.

As a part of the engagement with the private sector, the SSAs should have a strategy for working with their security partners on control systems security issues. This is particularly important if the sector faces the potential for significant risk if a control system were compromised. In most cases, the engagements are managed through the NIPP partnership framework and conduct public-private coordination and collaboration under the auspices of CIPAC. However, additional partnership and outreach through established control system groups and sector organizations may be appropriate to satisfy specific sector needs.

3.6.3 Information Sharing and Awareness

Unlike physical assets, many cyber systems are attacked on a regular basis. Control systems represent an attractive target because of the potential to cause physical harm to assets using cyber means. Sharing information on control system threats is an important function that requires trust and collaboration among key security partners and organizations. The NIPP assigns SSAs the role of exchanging cyber-specific information with sector security partners (including the international community, as appropriate) to improve the nation's overall cybersecurity posture.

The NIPP identifies four components of information sharing for cybersecurity: interagency coordination, information sharing and analysis centers, cybersecurity awareness for security partners, and cyberspace emergency readiness.

- Interagency coordination on control systems is accomplished through several means, including the Federal Partners, the CSCSWG, and programs such as the FBI's InfraGard.
- ISACs have been established in some sectors as a key resource for the sector partners to maintain situational awareness and receive threat information regarding cyber issues. The HSIN is also used by sector partners as an alternative or augmented resource to share information.
- Cybersecurity awareness is critical for the security partners. The Multi-State ISAC provides toolkits and outreach resources for general cybersecurity, control systems, and IT. DHS and SSAs are also working with sectors to expand control system security awareness. For example, the water sector has conducted eight regional Supervisory Control and Data Acquisition (SCADA)/IT summits to increase awareness of control systems security issues among chief information officers and IT departments. Additionally, the Chemical and IT Sectors are both participating in an Information Sharing Pilot under the CSCSWG in order to increase the flow and quality of information related to cybersecurity between the private sector, NCSD, and the SSAs.
- Cyberspace emergency readiness is provided through US-CERT, a continuous single point of contact for cyberspace warnings, analysis, incident response, and recovery. Security alerts are sent to security partners as they are discovered. The US-CERT Web site enables sector partners to report control system incidents and vulnerabilities in a secure information environment. US-CERT also provides a Web portal for a range of control system security resources, including assessment tools, training, information products, standards and references, and recommended practices.
- Daily, weekly, and monthly phone conferences are conducted by many of the ISACs and SSA's to share immediate information and other items of cybersecurity interest.

SSAs should work with their sector partners to integrate information sharing efforts and tailor them to fit the needs of the sector. SSAs should also build strong partnerships with their federal and sector counterparts to ensure rapid and trusted communications during emergencies and times of heightened alert.

3.6.4 Performance Measures and Reporting

A fundamental part of the NIPP Risk Management Framework is the continuous improvement to CIKR protection that is enabled by effective measurement of programs and activities designed to reduce risks. Developing useful measures of cyber and operational security is an important element of evaluating the overall risks, protective posture, and progress of each sector. Within companies, managers now use a variety of tools and methods to measure and assess their static security posture. In addition, researchers and technologists are working toward real-time security state monitoring techniques that can be used for all commercially available new and legacy systems.

Integral to these efforts is the identification of common metrics and risk assessment tools to help benchmark company performance and understand sector risks. Some of the challenges in assessing control system risks are the rapidly changing threat landscape, the discovery of new vulnerabilities, and the ability to evaluate scenarios that link threats to vulnerabilities to consequences. While there are no commonly accepted metrics or benchmarks for control system security, government and private sector organizations are working with utilities and industry partners to develop security standards and guidance, which will improve the ways control system risks are measured and support the development of meaningful security metrics. Several notable efforts are underway by NERC, NIST, the ISA, and the DHS Office of Infrastructure Protection. The results of these efforts provide guidance and measures for improving security and for regulatory compliance in the Energy and Chemical Sectors and for federal cyber assets.

The development of separate sector-specific metrics for control system security may not be appropriate for all sectors. However, it is recommended that each SSA work with its security partners to develop metrics for cybersecurity and determine whether separate metrics for control system security are warranted. The CIKR Sector Annual Report provides the mechanism for reporting on the progress in developing and collecting metrics that are suitable for each sector. In particular, sector-specific metrics are tailored to the unique characteristics of each sector and are used to assist in monitoring progress within the sector.

3.6.5 Research and Development Coordination

The development of new technologies offers one of the best long-term strategies for reducing control system risks. New technologies can help harden existing control systems and improve the protective capabilities of new systems by creating inherently safe and resilient networks or dramatically lowering the cost of existing capabilities.

The NIPP provides the overall framework for identifying and addressing R&D requirements to secure CIKR sector assets. The NIPP assigns DHS the responsibility to conduct and fund cybersecurity R&D in partnership with other SSAs and agencies. This R&D will provide new scientific understanding and technologies that can reduce risk to cyber systems. Control systems R&D is an integral component of all nine R&D themes identified in the NIPP, such as insider threat detection, intrusion detection and sensor systems, emerging threats and vulnerability analysis tools, and advanced infrastructure architecture. Significant R&D initiatives are currently underway throughout the federal government and the private sector to develop new technologies to improve control system security.

SSAs work in conjunction with DHS and their security partners to identify control systems technology requirements and determine if gaps exist between these requirements and current cybersecurity initiatives. Several SSAs, working with their sector partners, have made significant progress in identifying critical technology requirements and the gaps that must be addressed to achieve cybersecurity goals. For example, the energy sector, after completion of its control systems roadmap in 2006, launched *ieRoadmap*, an online roadmap that identifies and links over 100 R&D projects in government and industry to roadmap requirements. A public-private working group developed within the NIPP partnership framework, operating under the auspices of CIPAC and consisting of energy control systems experts, examines these projects to identify R&D gaps.

The NIPP Sector Annual Report provides the mechanism by which the sector reports on progress in finding and implementing solutions and identifies capability gaps. It enables the SSA and the sector to articulate its key cyber R&D requirements and provides input to DHS efforts to find collaborative solutions.

Developing Common Metrics

Implementing the NIPP to measure improvement and identify gaps requires risk assessment and metrics development. Sector-specific plans address performance goals and metrics at a high level, which means they are general in nature. The emerging sector-specific roadmaps more specifically address control systems. These roadmaps include goals, priorities and milestones to encourage stakeholders to take action to improve the cyber security posture on a voluntary basis. Government and industry technical, regulatory, and standards activities are also providing guidance to achieve some common approaches to risk assessment and the implementation of technologies to improve control systems security.

Some common vulnerabilities and mitigations to reduce the risk of cyber attacks have been publicized to increase awareness.[1,2,3] Some tools have also been developed that provide resources for private sector assessments using common security recommended practices and standards as their basis. The Control Systems Cyber Security Assessment Tool (CS2SAT) is an example of recent products in this area.

However, meeting the objective of common metrics to address the fundamental question of quantitatively measuring improvement in the security posture of a control system is complex. Many of the control systems standards and methodologies approach the topic from an operational safety and reliability viewpoint. From this view, analysts can judge or calculate improvements from knowledge of the frequency and consequence of failures in hardware or in control systems that fail to perform as described. The cybersecurity of intelligent control devices and networks falls outside the traditional methods for risk assessment. Cyber attacks can be multifaceted and present multiple approaches for common mode disruption of operations. As recognized by the CIKR stakeholders, IT cybersecurity approaches are not always available to owners and operators of control systems, and the frequency and sophistication of attacks are increasing. Assessments and corrective action products are likely to have limited effectiveness in this threat environment.

A gap exists in the availability of technical cybersecurity metrics. The development of such fundamentals can be a key resource in identifying specific measures that can regularly be used to assess effectiveness and by CIKR owner-operators in developing policies and strategies for the long term assurance of protection. Table 3-3 represents examples from a report[4] of a concept that defines security dimensions, ideals, and principles that can be used to develop quantitative measurements, goals, and effects.

Table 3-3. Dimensions of security, ideals, and related security principles.

Security Dimension	Ideal	Principle(s)
Security Group (SG) knowledge	SG knows current control system perfectly.	A. The system configuration should not be changed without the security group's knowledge. B. The system and its components should be evaluated and monitored for vulnerabilities.
Vulnerabilities	The control system has no vulnerabilities.	A. The time between vulnerability discovery and repair should be minimal. B. Complexity implies unknown vulnerabilities. C. Fix high-priority vulnerabilities first, with priority on vulnerabilities that can be exploited from the perimeter and that allow penetration. D. Credential keys should be strong, and should be changed regularly.
Recovery	SG can restore control system integrity instantly.	A. The time needed to restore the system with a previous uncorrupted version should be small. B. Several previous versions of system data should be saved regularly and protected from deliberate or accidental loss, such that in the event of compromise, a previous version can be chosen that is not likely to be corrupted.

1. NCSD Control Systems Security Program, Common Control System Vulnerability, INL/EXT-05-00993, November 2005, http://www.us-cert.gov/control_systems/pdf/csvul1105.pdf.
2. NCSD Control Systems Security Program, Control Systems Cyber Security Defense-in-depth Strategies, INL/EXT-06-11478, May 2006, http://csrp.inl.gov/Documents/Defense%20in%20Depth%20Strategies.pdf.
3. NCSD Control Systems Security Program, Standards and References, webpage visited June 4, 2008, http://www.us-cert.gov/control_systems/csstandards.html.
4. NCSD Control Systems Security Program, Control Systems Technical Security Metrics Report, December 2007.

3.7 Introduction of Strategy Elements

As outlined throughout this document (see Table 3.2 for summary), various stakeholder efforts exist for coordinating activities across a broad range of functions, organizations, and programs. The sector partnership framework of the NIPP supported by CIPAC provides the tools to provide an overall coordination of these efforts to achieve control systems security. Referring to Figure 3-4, a successful implementation process would bring stakeholders together to achieve the common vision.

The ICSJWG and ICS-CERT will facilitate coordination across federal and private sector partnerships for incident response and situational awareness activities. The roles of these two components as a strategy for overall coordination and the implementation activities required are discussed in Section 5.

Section 4 presents the coordination landscape and resources of stakeholder groups that comprise the context for these strategy elements.

The ICSJWG and ICS-CERT provide an umbrella coordinating mechanism to focus control system security efforts in order to achieve the desired end state as shown in Figure 3-6.

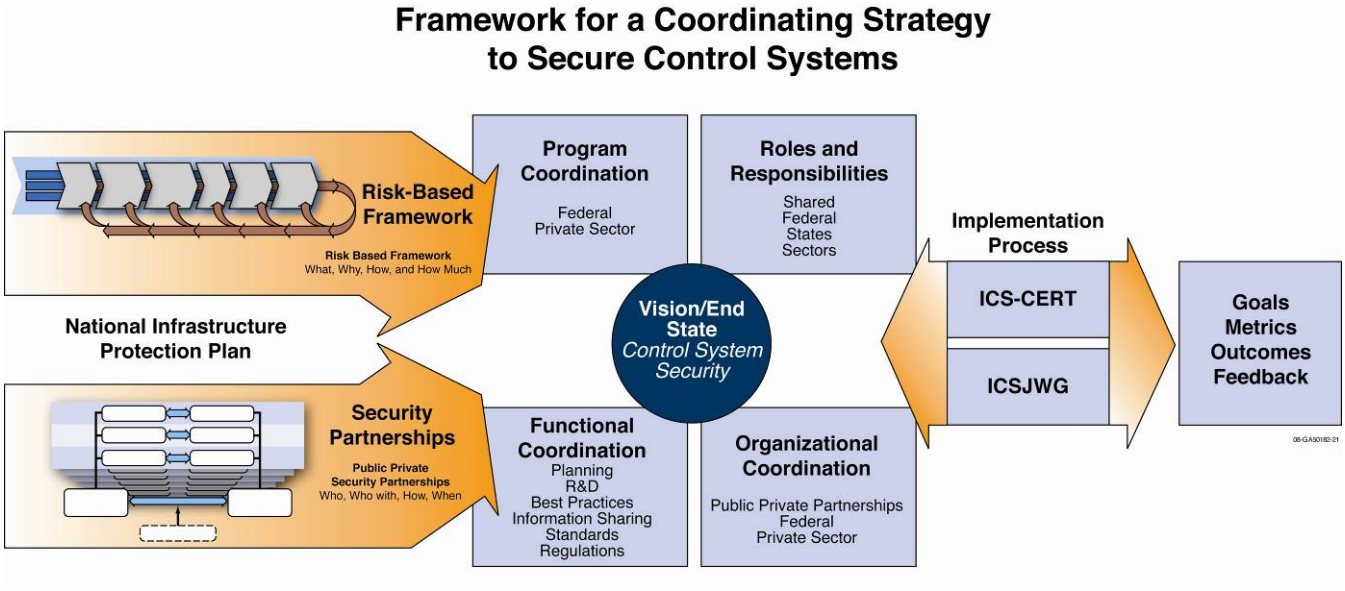


Figure 3-6. The ICS-CERT and ICSJWG as implementing strategy elements.

4. COORDINATION AND RESOURCE LANDSCAPE

A framework for coordination assumes that significant activity is ongoing among multiple and disparate organizations. Many efforts are underway within the CIKR stakeholder community to increase awareness and to develop security solutions commensurate with the complex nature of control system's risk from cyber attacks. Programs and activities within the sponsorship and participation of the public-private partnerships (and independently in industry) are increasing the opportunities for and the necessity to coordinate actions. The "coordination landscape" has been defined by these programs and activities where coordination influences the security posture. This same "landscape" also provides an approximation of the extent of resources committed to control systems security.

There are various GAO reports and several sector specific roadmaps that summarize many stakeholder programs. The following sections illustrate the depth and breadth of efforts affecting control systems security and the coordination present across sectors and stakeholders. It's important to note that multiple efforts are not necessarily duplicative and many already have program models which involve coordinating mechanisms.

4.1 Federal Efforts

Developing a strategy requires an understanding of current collaborative efforts and coordinating mechanisms. To develop this understanding from the federal perspective, an effort was initiated in FY 2006 to develop a forum for federal agencies to discuss control systems security as a federal working group. The result was the Federal Partners requested data from federal agencies with a stake in control systems security. In April and May of 2007 and 2008, agencies were contacted and queried for information on their current control systems activities, the objectives of those activities, and the mechanisms they use to coordinate with other agencies. The data call resulted in submissions from 28 agencies, of which 12 were SSAs.

This section provides an overview of the control systems programs and initiatives in the federal government, divided into four categories: NCSD, SSAs, mission and intelligence agencies, and federal control systems owners and operators. The roles and responsibilities of these agencies in securing control systems are detailed in Section 4.4. The coordinating mechanisms of these agencies in securing control systems are detailed in Appendix C.

Table 4-1 outlines the objectives of the control systems security activities performed by federal agencies, including SSAs, mission and intelligence agencies, and federal owner/operators.

Table 4-2 identifies the activities performed by federal agencies, including SSAs, mission and intelligence agencies, and federal owners/operators.

Table 4-1. Objectives of federal agency activities.

Threats		Vulnerability			Conse-quences			Oper-ations		Coord.	
Assess, analyze, and communicate threats	Other intelligence/counter intelligence	Measure/assess security posture	Develop, deploy protective measures	Sharing info/recommended practices	Consequence analysis	Detecting/mitigating incidents	Recover & reconstitution	Protect, operate, maintain Federal control systems	Acquisition, procurement of Federal control systems	Policy coordination	Partnership development

Table 4-2. Types of federal control systems cybersecurity activities.

Activity Type
Acquisition and Procurement
Assessments and Analyses
Intelligence Law Enforcement
Outreach and Information Sharing
Policy and Guidance Development
RDT&E and Related R&D
Recommended Practices and Training
Scenario Development
Standards
Support for Incident, Vulnerability, and Threat Management
Test Bed
Vulnerability Identification and Mitigation

4.1.1 DHS

As a federal department, DHS has several active responsibilities to coordinate control systems security activities and functions. These include the Protection and Outreach Division (POD), the S&T Directorate, and the National Cyber Security Division (NCSD).

In addition, DHS OIP (as the sector specific agency) is responsible for six CIKR sectors as well as compliance and regulatory functions for the chemical sector. IP coordinates with the GCC and SCC.

The S&T Directorate funds and coordinates research and development activities that include work in cyber and control systems security.

The lead agency for cybersecurity and control systems security activities is NCSD. NCSD was created by DHS to implement its responsibilities as outlined in the NSSC and HSPD-7. The CSSP mission is to provide cybersecurity leadership for the industrial control system community (for both private and governmental asset owners) and to assist NCSD in the implementation of its key responsibilities, as defined in the NIPP, for control system cybersecurity.

CSSP works to secure control systems from cyber attack coordinating efforts among federal, state, local, and tribal governments. CSSP also coordinates efforts with control system owners, operators, and vendors, to reduce the likelihood and severity of success of cyber attacks against critical infrastructure control systems.

The goal of the CSSP is to guide a cohesive effort between government and industry, and it achieves this through two objectives: providing guidance to the control systems community through a variety of mechanisms and activities; and working closely with public and private entities to establish effective partnerships with national laboratories, government entities and industry, as well as technical professionals across the control systems community through risk mitigation activities.

The objectives of CSSP activities are presented in Table 4-3. The types of activities CSSP will participate in are listed in Table 4-4.

4.1.2 Sector-Specific Agencies

Of the CIKR sector participants surveyed in the data call about their control systems security activities, 12 agencies responded. It is recognized that not all CIKR sectors perform control systems security activities, as some sectors do not recognize the risks that control systems have for the critical operation of the sector. The sectors who shared their control systems efforts were: defense industrial base; energy; government facilities; telecommunications; food and agriculture; chemical; commercial facilities; dams; emergency services; commercial nuclear reactors; materials; and waste, transportation systems, and water. Appendix C provides an overview of the objectives of the control systems security activities performed by each of the SSAs. Figure 4-1 offers a case study into a successful SSA.

Over 400 Partners Share Recommended Practices

The Department of Energy Office of Energy Reliability and Distribution National SCADA Test Bed (NSTB) program strengthens U.S. energy infrastructure through identification, mitigation, and communication of common cyber vulnerabilities within the electricity, oil and gas industries. The NSTB conducts cyber vulnerability assessments and develops mitigation techniques for industry partners. From the assessments, the NSTB is able to determine common vulnerabilities and to share this feedback with energy sector partners through standards organizations, training workshops, and conferences.

Government Contributors: DOE, Sandia National Laboratories, Idaho National Laboratory, Argonne National Laboratory, Pacific Northwest National Laboratory, Oak Ridge National Laboratory

Private Sector Contributors: ABB, American Transmission Company (ATC), LLC, AREVA T&D Automation, DTE Energy, GE Energy, Open Systems International, Inc., OSIsoft Inc., Siemens, Telvent

To Learn More: http://www.oe.energy.gov/nstb.htm

Figure 4-1. Case study.

4.1.3 Mission and Intelligence Agencies

Many other agencies within the federal government have responsibilities for security issues in control systems, or have taken on activities such as research, standards development, system testing, and support for control system operation. About 16 mission-related agencies contribute to the federal effort to secure control systems outside of the SSA duties. Some SSAs have additional mission-related efforts, and are included in both categories.

Table 4-3. Objectives of CSSP activities.

Threats	Vulnerability		Consequences		Coordination	
Assess, analyze, and communicate threats	Measure and assess security posture	Sharing information and recommended practices	Analysis consequences	Recover & reconstitution	Policy coordination	Develop partnerships

Table 4-4. Types of CSSP activities:

Activity Type
Standards support
Recommended practices and training
Acquisition and procurement
Develop control systems security requirements
Assessments and analysis
Outreach and information
Scenario development
Identification and mitigation vulnerability
Support management of incidents, vulnerabilities, and threats
Develop policy and guidance

Along with mission-related agencies (for example, FERC and NIST), some agencies perform intelligence operations in the realm of control systems security. These agencies include the CIA, FBI, and DOD. Mission-related agencies concentrate the majority of their activities on mitigating vulnerabilities and minimizing consequences, while intelligence agencies offer a unique set of capabilities aimed at threat deterrence by analyzing classified intelligence about real cyber threats.

Appendix C provides a summary of the control systems security activities performed by each of the mission and intelligence agencies.

4.1.4 Federal Owner/Operators

Agencies that own and operate control systems are tasked with implementing protective measures and investing in control systems security upgrades. All of the agencies surveyed responded that they assess, analyze, and communicate threats; detect and mitigate incidents; and protect and maintain federal control systems. However, these agencies often extend their duties by participating in R&D and by sharing information with federal agencies. These agency owner-operators perform a unique dual role in the efforts to secure control systems.

Appendix C provides a summary of the control systems security activities performed by each of the federal agencies.

4.2 Private Sector Efforts

This section summarizes the efforts being made to increase control system cybersecurity awareness and provide collaborative information to each of the CIKR sectors. Successful partnerships between government agencies and private sector entities require the establishment of mutually beneficial and trusted relationships. The relationships must be supported by a networked approach that provides timely access to information. The approach must also maintain business continuity by minimizing or managing risks while developing appropriate information sharing and analysis mechanisms within each sector. This will include supporting private sector coordinating mechanisms to facilitate the sharing of information on physical and cyber threats, vulnerabilities, incidents, recommended protective measures, and security-related practices.

Information sharing enables government and private sector partners to assess events accurately, formulate risk assessments, and determine appropriate courses of action. A number of organizations are collaborating to achieve this objective.

Therefore, a brief description of the private sector program organizations and an example of a coordinating mechanism used by the sector for communication is described below. The purpose of this communication outreach is to provide a voluntary security-related information sharing network amongst

the private sector stakeholders. Appendix D also describes the programs within each sector and the efforts currently underway to increase cybersecurity awareness. The efforts within each sector are summarized below.

4.2.1 Energy (Electricity, Oil, and Natural Gas)

The Energy Sector consists of a variety of privately owned organizations and businesses, which manage programs of trade, technology, regulatory standards, and information sharing. The stakeholders in this sector are also involved in R&D, exploration, production, distribution, and operation of electricity, oil, and natural gas systems, products, and services. Efforts underway in the Energy Sector to increase cybersecurity awareness include:

- Symposiums, forums, conferences, workshops, and meetings to bring researchers and practitioners together for discussion and training
- Assessments and analysis to identify strengths, vulnerabilities, and strategies
- Agreements and contracts to combine technologies, experience, and funding to facilitate security solutions.

Example of Energy Sector Coordinating Mechanism:

Program/Org	Description
North American Electric Reliability Corporation (NERC)	NERC is comprised of industry experts in the areas of cyber, physical, and operational security. NERC security initiatives are coordinated by Critical Infrastructure Protection Committee.

4.2.2 Water and Wastewater

The Water and Wastewater Sector consists of a variety of publicly and privately owned utilities and businesses involved in managing a vital natural resource, water. Members of these sectors maintain safe and reliable sources of drinking water, and properly treat and reclaim wastewater.

Efforts underway in the Water and Wastewater Sector to increase cybersecurity awareness include:

- A comprehensive and readily available online library that includes contaminant databases and resources about Water Sector vulnerabilities, incidents, and solutions for all hazards
- Training, related information, and referral services in wastewater, drinking water, and solid waste for small communities with populations up to 10,000
- Centralized database resources that gather, analyze, and disseminate threat information specific to the Water Sector.
- Regional meetings to disseminate and promote the implementation of their sector Roadmap for control system security

Example of Water and Wastewater Coordinating Mechanism:

Program/Org	Description
Water Environment Research Foundation (WERF)	WERF is dedicated to advancing science and technology that addresses water quality. Subscribers include individuals and organizations from municipal agencies, academia, government laboratories, and industrial and consulting firms.

4.2.3 Nuclear

The Nuclear Sector consists of privately and publicly owned organizations, technical bodies, regulatory agencies, standards bodies, and information sharing, programs, industry associations, and businesses. This sector's members are involved in the operation and maintenance of power production and materials test reactors, R&D, environmental risk, radiation waste, energy policy, and energy economics

Example of Nuclear Coordination Mechanism:

Program/Org	Description
Nuclear Energy Institute (NEI)	NEI is the policy organization of the nuclear energy and technologies industry and participates in both the national and global policy-making process. NEI ensures that policies promote beneficial nuclear energy uses and technologies around the globe.

4.2.4 Chemical

The Chemical Sector consists of businesses involved in transforming natural raw materials into commonly used products benefiting society's health, safety, and productivity. The chemical industry produces more than 70,000 products that are essential to automobiles, pharmaceuticals, food supply, electronics, water treatment, health, construction, and other necessities.

Efforts underway in the Chemical Sector to increase cybersecurity awareness include:

- Active participation in the CSCSWG and the associated Information Sharing Pilot.
- Implementation of RBPS 8, the cybersecurity standard associated with CFATS.
- Use of self-assessment tools by various stakeholders to measure security posture.
- Development of draft cybersecurity metrics through the CSCSWG Metrics Subgroup.
- Development of a cyber crisis communication process by ChemITC.
- Development of a Roadmap to Secure Control Systems in the Chemical Sector by a CIPAC working group.
- Awareness and educational activities sponsored by the National Petrochemical and Refiners Association Plant Automation and Decision Cybersecurity subcommittee

Example of Chemical Sector Coordination Mechanism

Program/Org	Description
Chemical Information Technology Center (ChemITC) of the American Chemistry Council (ACC).	ACC member facilities implement a complete, multilayered security program, developed by safety and security experts, that addresses site, transportation, and cybersecurity. ChemITC is a forum for companies in and associated with the ACC to address common IT issues and support the industry's ability to safely and efficiently deliver products essential to society

4.2.5 Dams

The Dams Sector comprises the assets, systems, networks, and functions related to dam projects, navigation locks, levees, hurricane barriers, mine tailings impoundments, and other similar water retention and/or control facilities. Dams are vital to the Nation's infrastructure and provide wide range of economic, environmental, and social benefits, including hydroelectric power, river navigation, water supply, flood control, and recreation.

The Dams Sector has interdependencies with a wide range of other sectors, including the:

- Agriculture and Food Sector, as a continued source of water for irrigation and water management
- Transportation Systems Sector uses dams and locks to manage navigable waters throughout inland waterways
- Water Sector, by supplying potable water to concentrated populations and commercial facilities in the United States.
- Energy Sector, by providing approximately 8 to 12% of the nation's power needs with hydropower dams
- Emergency Services Sector relies on Dams Sector assets for firefighting water supply, emergency water supply, and waterborne access in the event of a significant disaster.

Example of Dam Sector Coordination Mechanism

Program/Org	Description
Association of State Dam Safety Officials (ASDSO)	ASDSO is a national nonprofit organization serving state dam safety programs and the broader dam safety community, which includes federal dam safety professionals, dam owners and operators, engineering consultants, manufacturers, suppliers, academia, contractors, and others interested in improving dam safety.

4.2.6 Transportation

The Transportation Sector, which comprises all modes of transportation (aviation, maritime, mass transit, highway, freight rail, and pipeline), is a vast, open, interdependent networked system that moves millions of passengers and millions of tons of goods. Every day, the transportation network connects cities, manufacturers, and retailers, moving large volumes of goods and individuals through a complex network of approximately 4 million miles of roads and highways, more than 100,000 miles of rail, 600,000 bridges, more than 300 tunnels and numerous sea ports, 2 million miles of pipeline, 500,000 train stations, and 500 public-use airports. Example of Transportation Coordination Mechanism:

Program/Org	Description
Association of American Railroads (AAR) Operations Center	The AAR Operations Center collects, analyzes, and disseminates information on physical threats to railroad operations. It operates Railway Alert Network, through which AAR declares appropriate AAR freight railroad security alert levels.

4.2.7 ISACs

ISACs serve as central points of information sharing within some sectors and also act as the liaison to the federal government for operational security information sharing. Their main functions are to funnel vulnerability and threat information to companies and receive and collect information from companies.

Example of ISAC Coordination Mechanism:

Program/Org	Description
The Information Technology Information Sharing and Analysis Center (IT-ISAC)	IT-ISAC is a trusted community of security specialists from companies across the IT industry dedicated to protecting the IT infrastructure.

4.2.8 Information Technology and Communications

The Information Technology sector has identified their critical functions as providing: IT products and services; incident management capabilities; domain name resolution services; identity management and associated trust support services; Internet-based content, information, and communications services; and Internet routing, access, and connection services.

The Communication Sector is tightly coupled with the IT sector since many components in network and control are common. The sector is an integral component of the U.S. economy as it underlies the operations of all businesses, public safety organizations, and government. Over 25 years, the sector has evolved from predominantly a provider of voice services into a diverse, competitive, and interconnected industry using terrestrial, satellite, and wireless transmission systems. The transmission of these services has become interconnected; satellite, wireless, and wire line providers depend on each other to carry and terminate their traffic and companies routinely share facilities and technology with each other to ensure interoperability.

Many of these IT and communications functions are integral to large-scale, network-based control systems utilized across critical infrastructure sectors. Thus, private sector organizations that support IT/communications systems development, standards, applications, and operations are also relevant to control systems security issues.

Example of an Information Technology Coordination Mechanism:

Program/Org	Description
Information Technology Association of America (ITAA)	ITAA provides leadership in market research, standards development, business development, networking and public policy advocacy to some 350 corporate members doing business in the public and commercial sector markets.

4.2.9 Banking and Finance

The Banking and Finance Sector is a service-based industry providing a wide variety of financial services in the United States, and many such services throughout the world. These services range from the simple cashing of a check to highly complex arrangements that facilitate the transferring of financial risks. Financial institutions are organized and regulated based on the services the institutions provide. Therefore, the sector profile is best described by defining the services offered. These categories include: (1) deposit and payment systems and products; (2) credit and liquidity products; (3) investment products; and (4) risk-transfer products. With more than 17,000 depository institutions, 15,000 providers of various investment products, more than 8,500 providers of risk-transfer products, and many thousands of credit and financing organizations, the financial services sector is both large in assets and in the number of individual businesses.

Example of a Banking and Finance Coordination Mechanism:

Program/Org	Description
Financial Services Information Sharing and Analysis Center (FS-ISAC).	The FS-ISAC gathers threat, vulnerability, and risk information about cyber and physical security risks faced by the financial services sector. Sources of information include commercial companies who gather this type of information, government agencies, CERTs, academic sources, and other trusted sources. After analysis by industry experts, alerts are delivered to participants based on their level of service.

4.2.10 Postal and Shipping

The Postal and Shipping sector is comprised of the principal shippers of mail and packages such as the United States Postal Service, United Parcel Service, DHL, and Federal Express. This sector is

highly dependent on the IT, energy, telecommunications, and transportation sectors.

Example of a Postal and Shipping Coordination Mechanism:

Program/Org	Description
Sector Coordinating Council	The Postal and Shipping Sector has established a portal on the Homeland Security Information Network. This facilitates and enables information sharing between the SSA and private sector security partners, among Federal government agencies (GCC membership), between government and the private sector, and across other critical infrastructure sectors.

4.2.11 Emergency Services

This sector is largely governmental (federal, state, local, and tribal) applying resources to respond and mitigate natural and human caused events that impact public safety and lives. The sector recognizes that control systems can impact critical infrastructures and initiate catastrophic events requiring their response. The sector is interdependent to a number of other sectors (energy, communications, IT and telecommunications, transportation, and chemical) with these industry and trade associations involved in control systems security.

Example of an Emergency Services Coordination Mechanism:

Program/Org	Description
Emergency Management and Response-Information Sharing and Analysis Center (MNR-ISAC)	EMR-ISAC Goals is to promote awareness of the threats to and vulnerabilities of Emergency Service Sector (ESS) critical infrastructures, encourage ESS prevention, protection, and resilience actions for all disasters, and enhance the survivability, continuity, and "response-ability" in all-hazards environments.

4.2.12 Healthcare and Public Health

The Healthcare and Public Health Sector constitutes approximately 15% of the Gross National Product, equal to $1.86 trillion, and has an important impact on the U.S. economy. Privately owned and operated organizations comprise about 90% of the sector and identify themselves with the delivery of healthcare goods and services.

The public health component is largely composed of government agencies at federal, state, local, and tribal community levels. The public health component is not as large as the private component and performs a somewhat different array of functions, concentrating largely on preventive measures. The sector is highly diverse in its composition and relationships with its many systems, networks, services, facilities, functions, and roles, both public and private, needed to prevent disease and disability.

Example of a Healthcare and Public Health Coordination Mechanism:

Program/Org	Description
Healthcare Sector Coordinating Council (HSCC)	The mission of the HSCC is to coordinate plans, policy advice, and actions to preserve and restore the critical functions of the nation's healthcare delivery system and to support effective emergency preparedness and response to all hazards, including natural and manmade disasters.

4.2.13 Agriculture and Food

The Agriculture and Food sector represents extensive resources that provide for food production, processing, and distribution across the United States. The infrastructure includes over two million farms, nearly one million businesses, and as many facilities. Control systems are critical elements of food processing, packaging, and transportation.

Example of an Agriculture and Food Coordination Mechanism:

Program/Org	Description
Institute for Countermeasures against Agricultural Bioterrorism (ICAB)	ICAB was developed at Texas A&M University to help guard against biological agents designed to cause plant and animal disease.

4.2.14 Defense Industrial Base

The Defense Industrial Base (DIB) Sector includes components of DOD, other government agencies, and the private sector worldwide industrial complex that have capabilities to perform research and development, design, production and maintenance of military weapons systems, subsystems, components or parts to meet military requirements. The DIB Sector includes more than 100,000 companies and their subcontractors who perform under contract to DOD, and companies providing incidental materials and services to DOD, as well as government-owned

contractor-operated and government-owned government-operated facilities. DIB companies include domestic and foreign entities, some with operations located in many countries. The DIB Sector is dependent upon a number of other sectors, including Energy, Communications, and Transportation Systems.

The sector is divided into many segments, sub-segments, and commodities. Control systems apply to many of these segments and to the supply chain feeding them.

Example of a DIB Coordination Mechanism:

Program/Org	Description
National Defense Industrial Association (NDIA)	NDIA provides a legal and ethical forum for the interchange of ideas between the government and the defense industry.

4.2.15 Commercial Facilities

Facilities associated with the Commercial Facilities Sector 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. The majority of the facilities in this sector are owned and operated by the private sector, with minimal interaction with the federal government and other regulatory entities. The Commercial Facilities Sector consists of eight subsectors that include public assembly and sports areas, resorts, retail, real estate, theme parks, and retail centers. Control systems affect such critical areas as heating, ventilation, and air conditioning, security systems, and telecommunications.

4.2.16 National Monuments and Icons

This sector is comprised of primarily government or state owned facilities/assets with the Department of Interior as the SSA. The sector is interdependent to a number of other sectors and operations could be impacted by reduction of other sector services.

4.2.17 Government Facilities

The GFS includes a wide variety of facilities owned or leased by federal, state, local, or tribal governments, located domestically and overseas. Although some types of government facilities are exclusive to the GFS, government facilities also exist in most other sectors. Many government facilities are open to the public for business activities, commercial transactions, provision of services, or recreational activities and can be associated with other sectors. Other facilities not open to the public contain highly sensitive information, materials, processes, and equipment. Control systems are components of many government owned facilities, but may be included as key infrastructures in other sectors (energy: Bonneville Power Administration or Tennessee Valley Authority).

Example of a Government Facility Coordination Mechanism:

Program/Org	Description
Government Coordinating Council (GCC)	Government facilities are managed primarily by government agencies that are also the security partners. Educational facilities have additional state and local partners.

4.2.18 Critical Manufacturing

A new sector was recognized in 2008 to represent manufacturing capability that is considered part of the nation's critical infrastructure. The Critical Manufacturing Sector includes: Primary Metals Manufacturing, Machinery Manufacturing, Electrical Equipment Manufacturing, and Transportation and Heavy Equipment Manufacturing. The Critical Manufacturing SCC, SSA, and GCC have been organized and the Sector Specific Plan has been developed. The Critical Manufacturing Sector relies on a wide variety of industrial control systems that manage physical processes through computer-interface means. Cyber elements include electronic systems for processing the information necessary for management and operation or for automatic control of physical processes.

Example of a Critical Manufacturing Coordination Mechanism:

Program/Org	Description
National Association of Manufacturers	The nation's oldest and largest broad-based industrial trade *association*, represents 14000 companies in every industrial sector in every state

5. IMPLEMENTATION

Coordination occurs with critical infrastructure stakeholders as illustrated by the exhibits and discussion from the previous sections of this document. This coordination "landscape" is comprised of the many functions, stakeholders, and processes that further the implementation of technology and methods to improve control systems security. The GAO assessment and report recognized that while there are many activities aimed at improving security, a common vision or strategy was lacking to coordinate these efforts. The NCSD CSSP will lead the outreach and implementation of this strategy.

The NCSD was established by DHS to serve as the federal government's cornerstone for cybersecurity coordination and preparedness, including implementation of the National Strategy to Secure Cyberspace.

It is recognized that control systems security is a shared responsibility between owners/operators, vendors, systems integrators, academia, government, and the international community. The NIPP partnership framework provides the mechanisms for federal and private asset owners to coordinate activities in securing control systems through the SCC and GCC organizations for each sector. Therefore, CSSP works with the SCCs as they design specific plans, develop goals, and share control system security information within their sectors. The SSAs for each sector share this responsibility and provide guidance and coordination to assist stakeholders with control systems security implementation challenges. While CSSP is responsible for leading this coordination, the direct implementation of security practices and risk mitigation measures occurs at the stakeholder level.

The overarching control systems security strategy for the coordination of federal, state, and private industry security efforts will be achieved through two principle coordinating components operated and managed by CSSP: (1) the ICSJWG, cross-sector sponsored joint working group that uses a structured approach supported by the NIPP framework and the CIPAC, and (2) the expansion of the ICS-CERT for handling and responding to control systems related incidents.

5.1 The Industrial Control System Joint Working Group

The Industrial Control Systems Joint Working Group (ICSJWG) was created to coordinate control systems security initiatives and operate as a body within the NIPP partnership framework under the auspices of CIPAC.

Additional coordination mechanisms exist within the NIPP partnership framework. The NIPP partnership framework is supported by CIPAC, enabling implementation of public-private partnerships through derivative councils and working groups. Key among these are the SCCs and GCCs, whose members and affiliated entities also encompass the private sector cross-sector council (currently recognized as the PCIS), and the CSCSWG. These bodies, however, are broad in their coordination of infrastructure security matters and not specifically focused on control systems security. Prior to the formation of ICSJWG, the CSSP led informal groups of federal and private sector asset owners, operators, and vendors to discuss control systems issues.

The ICSJWG now provides a formal mechanism for the coordination of activities and programs across government and private sector stakeholders. The result is a forum for government and private sector partners to engage in a broad spectrum of critical infrastructure protection and resilience activities.

The ICSJWG consists of two subgroups; a government working group with members from the GCC, and an industry working group with members from the SCC who are focused on addressing cyber security issues affecting control systems. Since CIPAC is a coordinating mechanism directly supporting the NIPP partnership framework, members of the SCCs and GCCs may engage in joint CIKR protection-related discussions without violating the regulations of the Federal Advisory Committee Act.

The government working group under the ICSJWG leverages the Federal Partners and

sponsorship of the GCCs under the NIPP partnership framework. This fosters improved coordination of control system security issues, information sharing, and federal programs. Sponsorship of the private sector participation by the SCCs in the ICSJWG provides a more direct mechanism and partnership model which enables overall coordination across control systems security activities. This coordination allows participants to address efforts of mutual interest within various stakeholder communities, build upon existing efforts, reduce redundancies, and contribute to national and international CIKR security efforts.

5.2 Industrial Control System Cyber Emergency Response Team

The CSSP currently manages and operates the ICS-CERT in coordination with US-CERT. The ICS-CERT responds to and analyzes cyber threats and control systems incidents, conducts vulnerability and malware analysis, and provides onsite support for forensic investigations and analysis. The ICS-CERT shares and coordinates vulnerability information and threat analysis through actionable information products and alerts. The ICS-CERT provides more efficient coordination of control systems related security incidents and information sharing with federal, state, and local agencies and organizations, the Intelligence Community, private sector constituents including vendors, owners and operators, and international and private sector CERTS.

The CSSP is currently expanding upon these technical and response capabilities in order to further improve situational awareness, incident response, and vulnerability mitigation. This expansion encourages government and the private sector participation to report and share incident and vulnerability information. Trusted relationships provided by the ICSJWG, and through activities of the CSSP, are leveraged to increase and improve information sharing with the CIKR asset owner/operators and vendor community. The work is performed in conjunction with US-CERT and furthers their overall mission to coordinate defense against and response to cyber attacks across the nation.

5.3 Recommendations

To achieve this "overarching strategy" for the coordination of control systems security efforts across federal, state, local, and private sector stakeholders, current efforts need to be expanded upon to fully meet the expectations of Congress and fulfill the mission for control systems security. The creation of the ICSJWG for public-private coordination and collaboration within the NIPP partnership framework, and further enhancements to ICS-CERT capabilities will provide long-term strategic mechanisms for NPPD to coordinate efforts consistent with a 5–10 year vision of the protection of the nation's critical infrastructure control systems. The following sections describe how ICSJWG and ICS-CERT activities are interrelated and apply across organizational, functional, and program boundaries. These activities are consistent with many of the NIAC recommendations in the *Convergence of Physical and Cyber Security* (refer to Footnote 5) report and with the NCSD program strategy for control systems security.

5.3.1 ICSJWG Activities

The DHS CSSP created a working group focused on industrial control systems security in partnership with government and private sector entities within the NIPP sector partnership and operating under the auspices of CIPAC. This organization represents all 18 CIKR sectors and is comprised of GCC and SCC members as outlined by the NIPP. With the formalization of the ICSJWG, a structured partnership now exists that provides a forum within the government and private sector to address control systems security and mitigation challenges. The following activities are conducted by the ICSJWG in support of this strategy.

5.3.1.1 Provide leadership in development of control systems security principles

The ICSJWG will define cyber security principles associated with control systems as an important step in helping CIKR stakeholders frame security information, technology, and expertise. The proper application of these underlying principles is required to prevent, detect, mitigate, and recover from control systems security vulnerabilities. CSSP will provide leadership by developing the guiding principles for control systems security and analyzing the impact of trends and activities that could adversely affect the

integrity of control systems that automate much of the nation's critical infrastructure. These principles will be used as a guide for the SCCs and GCCs as they assess and secure the control systems within their sectors. The product and benefits of this effort can then be applied to many other coordinating efforts important to control system security.

5.3.1.2 Assume full engagement in the NIPP partnership for control systems security

As previously stated, the ICSJWG provides the mechanism for coordination across the federal, state, local, and private industry CIKR within the sector partnership framework defined by the NIPP. NCSD has been active in participation within the NIPP partnership framework in cybersecurity and is increasing its response to meet the mission in control systems cybersecurity. The following activities will enhance guidance and coordination of control systems security efforts:

- The ICSJWG will develop protocols and apply resources to organize subgroups to identify and resolve specific security issues related to control systems.
- SSAs will work with private sector partners to develop, update, and review SSPs and roadmaps that address control systems security issues in their specific CIKR sector.
- The CSSP will develop and implement the information sharing protocol for vulnerability disclosure and mitigation for CIKR control systems. This will include delineating the roles and interactions of all relevant stakeholders involved in this process, to include vulnerability researchers, disclosure sites, vendors, asset owners, and national CERTs.
- Under the NIPP partnership framework the ICS-CERT and ICSJWG will facilitate the exchange of threat information impacting control systems between relative stakeholders.

5.3.1.3 Maintain a high level of outreach and awareness within the CIKR stakeholder community

Outreach and awareness activities are a significant coordinating function across private industry and government stakeholders. Significant progress has been made with the CIKR stakeholders to identify issues and vulnerabilities in a distinct cyber aspect of control systems security versus IT. Outreach and awareness are long-term coordination efforts and are required to achieve continuous improvement in control systems security. Focused efforts are required in these areas:

- Increase control systems security awareness within industry, government and the international community by providing training and education opportunities. Develop training materials that will empower other SMEs and sector agencies to provide similar training opportunities on their own. This is particularly important in improving cybersecurity awareness among CIKR operations staff and corporate information security staff.
- Develop and provide recommended practices in coordination with private industry, which will integrate control systems security in the procurement, operation, and maintenance processes.
- Involve control systems vendors through a subgroup of the ICSJWG to develop solutions for security vulnerabilities in new and legacy systems.
- Encourage stakeholder involvement in the standards, trade, and professional organizations in developing and implementing consistent guidance for design, operation, and maintenance of control systems.

5.3.1.4 Advance performance measurement and feedback for control systems cybersecurity improvements in CIKR

An essential component of the NIPP process is the measurement and reporting of improvement in the protection of CIKR on a regular basis. Physical security threats in many cases have well defined solutions to protect CIKR. The application and measurement of success for solutions to control systems security vulnerabilities is complex. Technology, standards, policies, and metrics are all components of the solution space for control systems security. As a part of the NIPP response, industry and government will provide updates on progress as part of the Sector Annual Report. DHS seeks to improve the coordination and quality of reporting through the following activities:

- Work with industry to improve, develop, and streamline common cyber requirements for performing critical infrastructure assessments.
- Coordinate with security providers and evaluators to enable them to perform consistent control systems cybersecurity assessments. These assessments leverage recommended common methodologies to provide results that are more consistent across CIKR facilities and sectors.
- Coordinate with CIKR owner-operators and the vendor community to support testing and validation of vulnerabilities and assessment processes to demonstrate performance improvement and mitigation of viable threats to control systems.
- Participate with standards bodies to improve control systems industry standards both nationally and internationally to promote a coordinated approach for the protection of CIKR.

5.3.1.5 Coordinate and participate in the identification and analysis of gaps in control systems security technologies, policies, and planning

There are areas where activities are required to provide assurance of the success of control system security efforts. As sector specific plans and security roadmaps evolve, more gap analyses will be performed to assist in prioritization and identification of where new efforts are needed. As outlined in the *National Strategy for Securing Cyberspace*, DHS has a significant role as sponsor, coordinator, and/or facilitator of these efforts as part of their mission to secure cyberspace. In support of DHS's mission NCSD will:

- Actively participate in the review, analysis, and feedback provided by the Sector Annual Reports for control systems security input. This input will be coordinated with other government and private sector stakeholders that provide data to this report as their participation warrants.
- Analyze results of control systems cybersecurity assessments with CIKR stakeholders to identify gaps in protection and mitigation solutions. Such gaps that do not have short-term solutions available to the stakeholders will be considered for action from programs that provide assistance for technology development. Cooperation between appropriate stakeholder organizations, including federal programs and SSAs, to determine a plan for mitigation of the security vulnerability or gaps is essential for a consistent approach to security.
- Coordinate efforts within the government and private sector partnerships to determine a process by which accreditation and certification of systems, vendors, and security professionals can be developed. This will help to address the needs of stakeholders by increasing the assurance of control systems cybersecurity. Accreditation and certification are topics that have the interest of many CIKR owner operators and the vendor community. These are methods utilized in the IT community to address security posture and preparedness within information systems infrastructure and of their IT security and management professionals.

5.3.2 ICS-CERT Activities

Managed and operated by the CSSP, the ICS-CERT is a complement to the US-CERT, extending the current control systems security technical and response capabilities. The ICS-CERT collaborates with and supports US-CERT in its mission with a focus on critical infrastructure control systems and networks. The following activities are conducted by the ICS-CERT in support of this strategy.

5.3.2.1 Increase CIKR control systems security participation and role in incident response/information sharing

The primary response capability for cyber incidents is provided through the US-CERT; established as part of the *National Strategy for Securing Cyberspace*. Control systems security situational awareness and vulnerability discovery has evolved with NCSD programs and collaboration with other federal and private industry activities. Incident response, information sharing, and mitigation and recovery are critical components of a strategy to secure control systems for CIKR. The ICS-CERT coordinates control systems related incidents, response and information sharing efforts across federal, state, local, and private sector activities and will:

- Enhance threat and risk assessment capabilities through formal program relationships and in coordination with the Intelligence Community and its member agencies and the DHS Office of

Intelligence and Analysis (I&A), responsible for ensuring that information related to homeland security threats is collected, analyzed, and disseminated to the full spectrum of homeland security customers.

- Conduct control systems-related situational awareness activities, vulnerability assessments, malware analysis, onsite forensic investigation and event analysis capabilities, and consequence impacts to critical infrastructure by leveraging coordination with other agency efforts, public sector relationships, and information sources.
- Coordinate with the Intelligence Community to develop threat briefings to private sector CIKR owner operators to facilitate the business case for adoption of advances in technology and policies that reduce risk to control systems in CIKR.
- Develop and implement protocols for CIKR control systems vulnerability identification and disclosure with coordination and/or validation procedures.
- Coordinate vulnerability discovery and validation efforts to advance technology and R&D efforts in the federal and private sector through the ICSJWG and other working groups implemented under the NIPP partnership framework and operating under the auspices of CIPAC.
- Coordinate supply chain efforts for control systems security in the federal and private sectors.
- Extend control systems security response capabilities for deployment in an integrated fashion with US-CERT and the GFIRST community. NCSD currently coordinates incident response and awareness activities with CIKR stakeholders and participates in national exercises, such as Cyber Storm to ensure operational preparedness.
- Engage the international community to identify and achieve common goals and objectives that lead to a higher level of security in CIKR control systems. Training, situational awareness, testing and analysis methodologies, and joint exercises will be pursued with the trusted international partners.
- Coordinate and address mitigation measures across all sectors by understanding the operational impact of these interdependencies. Addressing interdependencies requires a systematic and holistic approach with involvement and input from the control system community. Focusing solely on the vital functions that control systems provide within a sector overlooks the importance of the independencies among the sectors.

5.4 Performance Measures

The rapid pace of change in cyber technologies combined with the uncertainty in markets, regulations, and risk require that critical infrastructure sectors stay vigilant and responsive to a variety of plausible futures. As NPPD pursues the strategies contained in this document, it must review, assess, and adjust the coordination activities that will lead to success today and in the future. NCSD will regularly assess the coordinating activities defined in the *Strategy* and highlight progress as part of its reporting process, or as required by DHS. The Strategy may also be updated as necessary to ensure alignment with the NIPP and ongoing efforts.

This page intentionally left blank

6. CONCLUSION

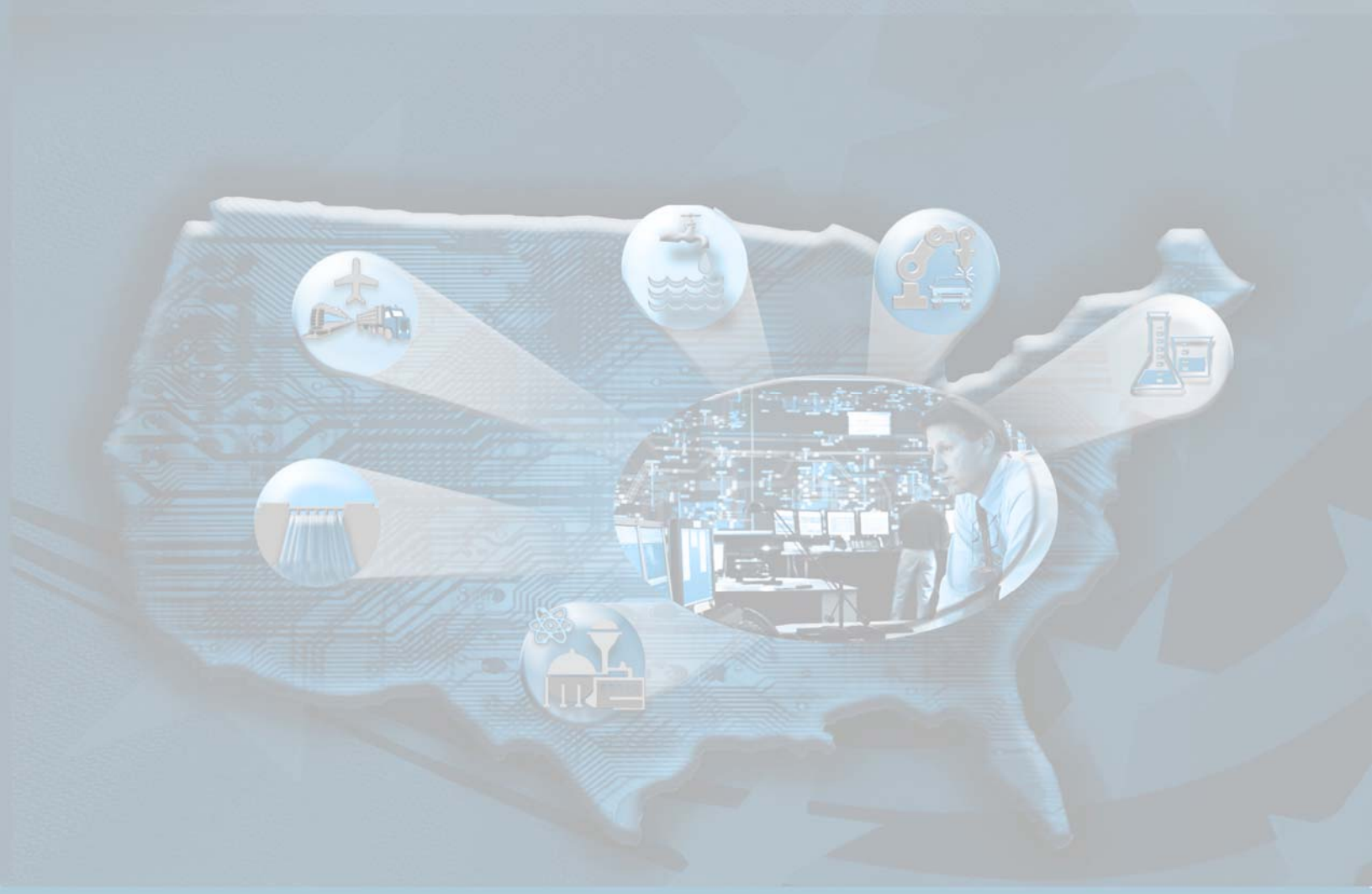
Control systems cybersecurity and critical infrastructure protection are tightly interrelated. Government and private sector stakeholders are increasingly aware that "security through obscurity" or assumptions that it is too difficult to exploit control systems cyber vulnerabilities are invalid. This awareness is also increasing within adversary communities as vulnerabilities and exploits, once targeted for financial gain, can be demonstrated to impact cross sector critical infrastructures. The increasing attention within the stakeholder community to address this issue has also strengthened programs and activities within the government and industry. Multiple efforts within these organizations and through partnerships are providing the needed focus to incrementally advance security in control systems through better policies, information sharing, and mitigation processes. Technology development that provides a longer-term view of protection and mitigation is also evolving in response to industry and government involvement.

The establishment of the NIPP sector partnership provides the framework for key coordinating mechanisms through the partnership model and the participation of critical infrastructure stakeholders. This framework in action defines the "coordination landscape" in which organizations can operate to address and leverage security requirements, solutions, resources, and planning.

A coordinating strategy that leverages this framework is of value if it focuses on the key security principles to assess control systems cybersecurity and the barriers and gaps that impact the advancement of security across all sectors. The key components of the *Strategy*, the ICSJWG and ICS-CERT, provide DHS with the mechanisms for coordinating partnerships and stakeholder efforts to effectively manage cybersecurity risk. Through these two components, NCSD will significantly advance its mission to secure cyberspace and America's cyber assets to include control systems security within critical infrastructure.

The implementation of the Strategy supports DHS in its role to guide efforts as fully engaged participants in the NIPP partnership framework, providing leadership and guidance to government and industry stakeholders, and supporting effective partnerships with federal agency programs to achieve common goals.

Similar to the NIPP, the *Strategy* is a long-term view for DHS. The value derived from its implementation will be measured in the effectiveness of preventing, deterring, and responding to cyber attacks on control systems within critical infrastructure.



Appendix A

Authorities and References

This page intentionally left blank

Appendix A
Authorities and References

This appendix summarizes authorities and references extracted from Appendix 2A of the *National Infrastructure Protection Plan* (NIPP)[A-1] that support the coordination *Strategy to Secure Control Systems*. Though not all inclusive, these summaries reflect the authorities most specific to those entities with vested interest in control systems security. Discussion is added to provide control systems security relevance.

AUTHORITIES

A1.1 Statues

Homeland Security Act of 2002

The Homeland Security Act of 2002 establishes a Cabinet-level department headed by a Secretary of Homeland Security with the mandate and legal authority to protect the American people from the continuing threat of terrorism. In the Homeland Security Act of 2002, Congress assigns the following primary missions to the Department of Homeland Security (DHS):

- Prevent terrorist attacks within the United States.
- Reduce the vulnerability of the United States to terrorism at home.
- Minimize the damage and assist in the recovery from terrorist attacks that occur.
- Ensure that the overall economic security of the United States is not diminished by efforts, activities, and programs aimed at securing the homeland.

This statutory authority defines the protection of critical infrastructure and key resources (CIKR) as one of the primary missions of the Department. Among other actions, the act specifically requires DHS to:

- Carry out comprehensive assessments of the vulnerabilities of the CIKR of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks.
- Develop a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including power production, generation, and distribution systems; information technology and telecommunications systems (including satellites); electronic financial and property record storage and transmission systems; emergency preparedness communications systems; and the physical and technological assets that support such systems.
- Recommend measures necessary to protect the CIKR of the United States in coordination with other agencies of the federal government and in cooperation with State and local government agencies and authorities, the private sector, and other entities.

Discussion: *This Act is the seminal law creating DHS and defining critical infrastructure and plans required for its protection. Control systems are mentioned briefly in the context of insider threats and discovery of information, such as vulnerabilities, that may allow an attacker to disrupt critical operations.*

Critical Infrastructure Act of 2002

Enacted as part of the Homeland Security Act of 2002, the Critical Infrastructure Act of 2002 creates a framework that enables members of the private sector and others to voluntarily submit sensitive information regarding the nation's CIKR to DHS with the assurance that the information, if it satisfies certain requirements, will be protected from public disclosure.

The PCII Program, created under the authority of the Act, is central to the information-sharing and protection strategy of the NIPP. By protecting sensitive information submitted through the program,

1. *National Infrastructure Protection Plan*, Department of Homeland Security, 2006, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

the private sector is assured that the information will remain secure and only be used to further CIKR protection efforts.

Discussion: *Information sharing, particularly involving site-specific data and incidents, is a significant issue when working within public-private security partnerships. The PCII program is being promoted to assist in this sharing within the private sector. In control systems security applications, this information would include sensitive, proprietary configurations, operating processes, consequences of loss, and incident data. DHS and other sector-specific agencies (SSAs) with access to this information can develop a realistic picture of risk for sectors, which will aid in coordination and collaboration with the private sector to reduce these risks.*

Cyber Security Research and Development Act of 2002

The Cyber Security Research and Development Act of 2002 allocates funding to National Institute of Standards and Technology (NIST) and the National Science Foundation (NSF) for the purpose of facilitating increased research and development (R&D) for computer network security and supporting research fellowships and training. The act establishes a means of enhancing basic R&D related to improving the cybersecurity of CIKR.

Discussion: *NIST and the NSF are involved in funding and supporting R&D in technologies related to control systems security. Computer network security is an essential component of modern and emerging control systems technology and will be a nexus for risk reduction solutions Coordination with these entities and with other agencies, including DHS funded research, is an objective of the strategy.*

Intelligence Reform and Terrorism Prevention Act of 2004

The Intelligence Reform and Terrorism Prevention Act of 2004 provides sweeping changes to the U.S. Intelligence Community structure and processes and creates new systems specially designed to combat terrorism. Among other actions, the act:

- Establishes a Director of National Intelligence with specific budget, oversight, and programmatic authority over the Intelligence Community.
- Establishes the National Intelligence Council and redefines "national intelligence."
- Requires the establishment of a secure ISE and an information-sharing council.
- Establishes a National Counterterrorism Center, a National Counter Proliferation Center, National Intelligence Centers, and a Joint Intelligence Community Council.
- Establishes, within the Executive Office of the President, a Privacy and Civil Liberties Oversight Board.
- Requires the Director of the Federal Bureau of Investigation (FBI) to continue efforts to improve the intelligence capabilities of the FBI and to develop and maintain, within the FBI, a national intelligence workforce.
- Directs improvements in security clearances and clearance processes.
- Requires DHS to develop and implement a national strategy for transportation security and transportation modal security plans; enhance identification and credentialing of transportation workers and law enforcement officers; conduct R&D into mass identification technology, including biometrics; enhance passenger screening and terrorist watch lists; improve measures for detecting weapons and explosives; improve security related to the air transportation of cargo; and implement other aviation security measures.
- Directs enhancements to maritime security.
- Directs enhancements in border security and immigration matters.
- Enhances law enforcement authority and capabilities and expands certain diplomatic, foreign aid, and military authorities and capabilities for combating terrorism.
- Requires expanded machine-readable visas with biometric data; implementation of a biometric entry and exit system, and a registered traveler program; and implementation of biometric or other secure passports.

- Requires standards for birth certificates and driver's licenses or personal identification cards issued by states for use by federal agencies for identification purposes, and enhanced regulations for social security cards.
- Requires DHS to improve preparedness nationally, especially measures to enhance interoperable communications, and to report on vulnerability and risk assessments of the Nation's CIKR.
- Directs measures to improve assistance to and coordination with state, local, and private sector entities.

Discussion: *Coordination and sharing of information on threats within intelligence, law enforcement, and SSAs for control systems security was recognized by the National Infrastructure Advisory Council (NIAC) as an area that needed additional effort. The last two bullets of the summary are relevant to coordination of control systems risk assessment activities within the security partnerships.*

A1.2 National Strategies

National Strategy for Homeland Security (July 2002)

The *National Strategy for Homeland Security* establishes the nation's strategic homeland security objectives and outlines the six critical mission areas necessary to achieve those objectives. The *Strategy* also provides a framework to align the resources of the federal budget directly to the task of securing the homeland. The *Strategy* specifies eight major initiatives to protect the nation's CIKR, one of which specifically calls for the development of the NIPP.

Discussion: *Protection for Control systems infrastructure is included under the umbrella of several major initiatives in the critical mission area of Protecting Critical Infrastructure and Key Assets. Subsequent national policy and strategy documents along with the NIPP provide the specific framework for coordination of control systems security efforts.*

National Strategy to Secure Cyberspace (February 2003)

The *National Strategy to Secure Cyberspace* sets forth objectives and specific actions to prevent cyber attacks against America's CIKR, reduce nationally identified vulnerabilities to cyber attacks, and minimize damage and recovery time from cyber attacks. The strategy provides the vision and serves as the foundation for the cybersecurity component of CIKR.

Discussion: *This document provides the first significant recognition and inclusion of control systems security as a major initiative and coordination opportunity with other SSAs such as the DOE. DHS is the lead agency for cybersecurity initiatives. Most of the general elements in the coordination strategy such as risk reduction (threat, vulnerability, and consequence), information sharing and awareness; partnerships, research and development, and response and preparedness have major visibility in the national strategy.*

A1.3 Planning Documents

DHS Strategic Plan 2004

This *Strategy* sets forth seven high-level goals and supporting objectives for DHS along with the organizational structure for implementation. The *Strategy* follows their mission directed by the *National Strategy for Homeland Security*.

Discussion: *Control systems security is generally recognized in the protection goal and the objective to reduce vulnerabilities. This same goal and objective identifies the national protection plan to protect physical and cyber infrastructure.*

National Response Plan of 2004

The National Response Plan of 2004 (NRP) is an all-discipline, all-hazards plan that establishes a single, comprehensive framework for the management of domestic incidents. It provides the structure and mechanisms for coordinating federal support to state, local, and tribal incident managers and for exercising direct federal authorities and responsibilities. The NRP assists in the important homeland security mission of preventing terrorist attacks within the United States; reducing the vulnerability to all natural and manmade hazards; and minimizing the damage and assisting in the recovery from any type of incident that occurs.

Discussion: *The NRP Cyber Incident Annex provides the scope, policies, and conduct of operations for a cyber incident that would include exploits of control systems and impacts to critical infrastructure. The NRP assigns the DHS National Cyber Security Division as a lead coordinating agency. A number of response organizations come into play such as the National Cyber Response Coordinating Group, US-CERT, Intelligence Community—Incident Response Center, and the Department of Defense Joint Task Force—Global Network Operations center. These organizations coordinate subject matter expert response resources, including control systems subject matter experts for analysis and mitigation.*

DHS Science and Technology Strategic Plan (2007)

The DHS Science and Technology Strategic Plan defines how the directorate identifies priorities, goals, objectives, and policy for coordinating the federal government's civilian efforts to identify and develop scientific solutions and technological countermeasures to address a wide variety of terrorist and natural threats to the homeland.

Discussion: *This strategic plan provides a high-level overview of the organization and process for coordination work across many disciplines and mission areas. Cybersecurity (including control systems) is included in one of the technical divisions (Command, Control, and Interoperability). Coordinating mechanisms within government-private partnerships are referenced within other organizational areas.*

A1.3 Homeland Security Presidential Directives

HSPD-1—Organization and Operation of the Homeland Security Council (October 2001)

HSPD-1 establishes the Homeland Security Council (HSC) and a committee structure for developing, coordinating, and vetting homeland security policy among executive departments and agencies. The directive (1) provides a mandate for the HSC to ensure the coordination of all homeland security-related activities among executive departments and agencies and (2) promotes the effective development and implementation of all homeland security policies. The HSC is responsible for arbitrating and coordinating any policy issues that may arise among the different departments and agencies under the NIPP.

Discussion: *The creation of the HSC provides a high-level court for coordination across the government. While the current coordinating strategy is designed to be a descriptive, not prescriptive document, it is feasible that future versions may have recommendations affecting the policies and plans of other SSAs.*

HSPD-7—Critical Infrastructure Identification, Prioritization, and Protection (December 2003)

HSPD-7 establishes a framework for federal departments and agencies to identify, prioritize, and protect CIKR from terrorist attacks, with an emphasis on protecting against catastrophic health effects and mass casualties. This directive establishes a national policy for federal departments and agencies to identify and prioritize United States CIKR and to protect them from terrorist attacks. HSPD-7 mandates the creation and implementation of the NIPP and sets forth roles and responsibilities for DHS; SSAs; other federal departments and agencies; and state, local, tribal, private sector, and other security partners.

Discussion: *This directive affirms DHS as the lead agency in cybersecurity for which control systems security is an element. The direction to create and implement the NIPP provides more specific authorities that apply to coordination roles and responsibilities for control system security.*

A1.4 Other Authorities

Executive Order 13231—Critical Infrastructure Protection in the Information Age (October 2001) (amended by E.O. 13286, February 28, 2003)

Executive Order 13231 provides specific policy direction to ensure protection of information systems for critical infrastructure, including emergency preparedness communications and the physical assets that support such systems. It recognizes the important role that networked information systems (critical information infrastructure) play in supporting all aspects of our civil society and economy and the

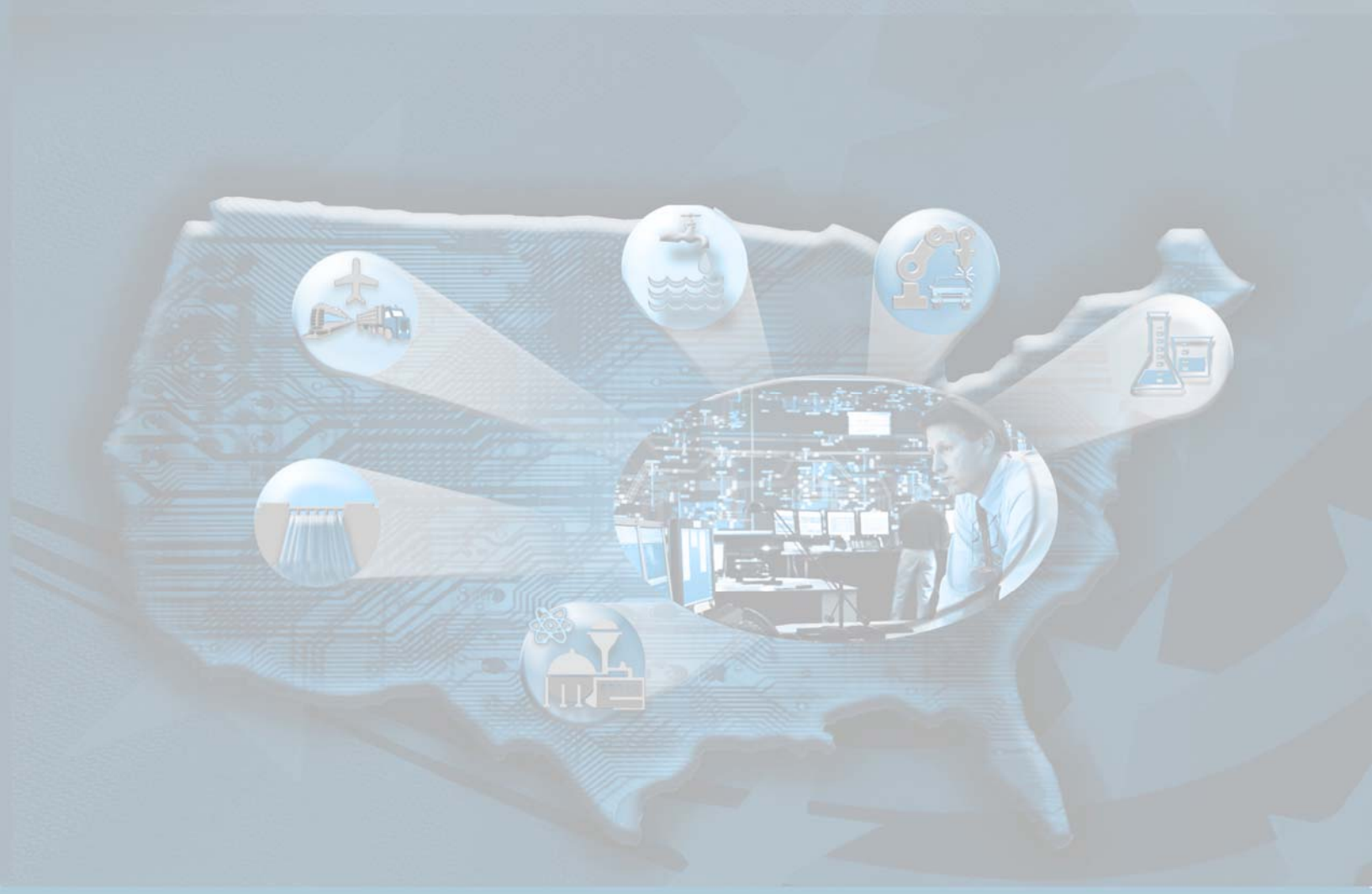
increasing degree to which other critical infrastructure sectors have become dependent upon such systems. It formally establishes, as United States policy, the need to protect against disruption of the operation of these systems and to ensure that any disruptions that do occur are infrequent, of minimal duration, manageable, and cause the least damage possible. The Executive order specifically calls for the implementation of the policy to include "a voluntary public-private partnership, involving corporate and nongovernmental organizations." The order also reaffirms existing authorities and responsibilities assigned to various executive branch agencies and interagency committees to ensure the security and integrity of federal information systems generally and of national security information systems in particular.

National Infrastructure Advisory Council

Executive Order 13231 (as amended by E.O. 13286 of February 28, 2003, and E.O. 13385 of September 29, 2005) also established the NIAC as the President's principal advisory panel on critical infrastructure protection issues spanning all sectors. The NIAC is composed of not more than 30 members, appointed by the President, who are selected from the private sector, academia, and state and local government, representing senior executive leadership expertise from the critical infrastructure and key resource areas as delineated in HSPD-7.

The NIAC provides the President, through the Secretary of Homeland Security, with advice on the security of critical infrastructure, both physical and cyber, supporting important sectors of the economy. It also has the authority to provide advice directly to the heads of other departments that have shared responsibility for critical infrastructure protection, including United States Department of Health and Human Services, Department of Transportation, and DOE. The NIAC is charged to improve the cooperation and partnership between the public and private sectors in securing critical infrastructure and advises on policies and strategies that range from risk assessment and management, to information sharing, to protective strategies and clarification on roles and responsibilities between public and private sectors.

Discussion: *The NIAC working group on the Convergence of Physical and Cyber Technologies and Related Security Management Challenges developed a report and recommendations (January, 2007) that provided insight as to how to remove barriers and promote coordination of efforts in key control systems security activities.*



Appendix B

Control Systems Risk

This page intentionally left blank

Appendix B—Control Systems Risk

Securing critical infrastructure necessitates securing control systems. As integral components of critical infrastructure, control systems monitor and control sensitive processes and functions used in facilities that generate, transmit, and distribute electricity; process chemicals; refine petroleum; and treat and supply drinking water.

Reports from the last several years show a steady increase in general cyber threats that pose security risks to these control systems. Factors contributing to this escalation include (1) the adoption of standardized technologies, (2) increased connectivity of control systems to other networks, (3) insecure remote connections, and (4) the widespread availability of technical information about control systems and their vulnerabilities. Although, to date, it has not been possible to quantify the risk of potential cyber attacks on control systems tied to critical infrastructure/key resource (CIKR), the concern has been qualitatively stated in a number of prior references.[1,2,3,4,5]

Definition of Risk

Risk is the projected (or expected) loss from a future sequence of events with an unwanted outcome. Neither the losses nor the attack event need actually to have occurred in the past. Risk is further defined as the product of the consequences (i.e., the loss) of that event times the probability of that loss occurring.

The total system risk is the summation of the risks from all possible events. A single event may have many different consequences. There may be many potential events arising from one or many threats, and initiating action may lead to many sequences of actions which in turn have many possible outcomes. A description of such event sequences is referred to as "risk scenarios."

When both probability and consequence can be quantified, either based on historical accounting of a large number of similar events, or from detailed analytical prediction, risk is immediately known in terms of annualized cost in terms of dollars and health impacts. The probability of any risk scenario involving a terrorist attack, however, is effectively unknown; and predicting isolated and rare events is generally accepted as virtually impossible to calculate.

Therefore, DHS, in the National Infrastructure Protection Plan (NIPP) develops the basis for risk as a function of threat, vulnerability, and consequence. Threat and vulnerability (both very qualitative terms) are used to represent probability without specifying the mathematical formalism. Often, risk analysts will include a term to represent the defense of recovery of the system, such that the greater the defense, or speed of recovery, the lower the risk. The NIPP framework assumes that defense and recoverability are included in the vulnerability term. That description of risk is accepted in this document.

In spite of the difficulty of quantifying risk, an economically efficient risk management strategy requires a reasonable quantitative estimate of future risk. A rationally responsive system would attempt to commit fewer resources to reduce risk than the annualized value of that risk. Ultimately, decisions to invest in a certain level of countermeasures to protect against cyber attack risk are made with or without quantified risk values. The stronger the objective bases for those decisions the better (more efficiently) will those decisions be accepted and successfully implemented.

Threats and Vulnerabilities

A successful cyber attack on a control system could endanger public health and safety, damage the environment, or cause a loss of production, generation, or distribution of public utilities. A more complete list of causes for increasing vulnerability is shown in the text box at the right.

A succinct summary of the technical bases and trends for risk of cyber attack to control systems is presented in the July 2005 Informational Focus Paper, "Control Systems Cyber Security Awareness,"[Ref 5] produced by the United States Computer Emergency Readiness Team (US-CERT).

Past and Current Threats

Figure B-1 graphically depicts the timing and types of threats over almost 30 years.

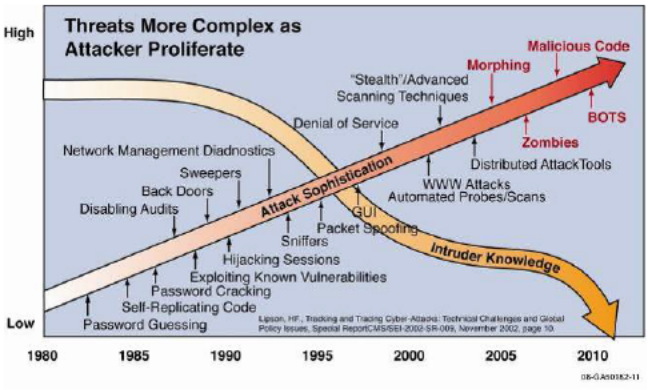


Figure B-1. Threat trends over 30 years.

Of particular concern is the fact that attack sophistication is increasing while knowledge needed to successfully execute an attack is decreasing. This is problematic for control systems because many utilities still use legacy systems, which lack the defenses required for the scope and severity of modern-day attacks. Due to the rapid integration of technology and networks between corporate IT and control systems, there is now a substantial gap between the capacity for attacks against control systems and the ability to defend control systems against them.

Causes for increased vulnerabilities:

- Increased connectivity
- Interdependencies
- Increased access and vulnerabilities due to complexity
- Continued presence of insecure legacy systems
- Increased system accessibility from internet and wireless
- Increased use of commercial off the shelf products
- Increased information availability
- Increased complexity of attacks
- Decreased skill level needed to attack

Another view of the threat picture is shown in Figure B-2 where, the various threats are plotted against consequences and likelihood. Also identified are the various types of threat agents (hackers, nation states, etc.) most likely to execute these threats. The likelihood of the kind of attacks typically executed by these various threat identities does not change, but the consequences can change dramatically.

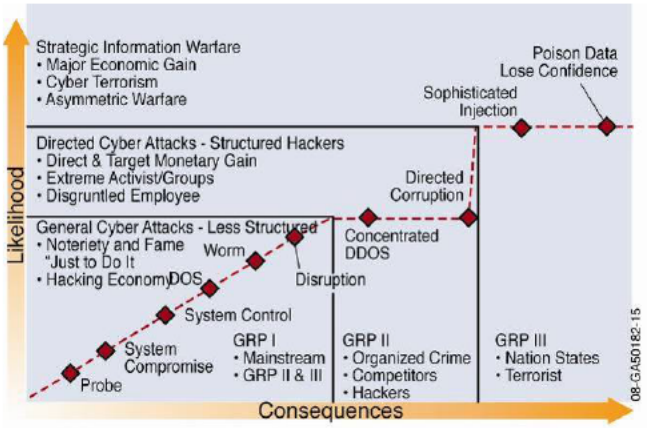


Figure B-2. Qualitative cyber threat—consequence function.

Vulnerabilities

A document published by the North American Electric Reliability Corporation (NERC) [6] specifically describes 10 major vulnerabilities related to common vulnerabilities that exist throughout the control system landscape.

Two other complementary efforts are underway to identify new and emerging control systems' vulnerabilities and share associated information.

The US CERT Website[7] provides an instructive overview of the general types of vulnerabilities for control systems. US-CERT also publishes information about a wide variety of vulnerabilities (see Figure B-3); those that meet a certain severity threshold are described in Technical Cyber Security Alerts.[8] These alerts include technical descriptions of the vulnerability; impacts, solutions, and workarounds; and lists of affected vendors. This information is also entered into the National Vulnerability Database.[9]

Figure B-3. US-CERT posted vulnerabilities.

The National Cyber Security Division Control Systems Security Program publishes a quarterly trends and analysis report that presents a review and analysis of the quarter's most significant control system security events and interest level indicators. It includes analyses of characteristics and trends, giving special attention to those vulnerabilities with the highest risk. This information is reported to the federal control systems security community and critical infrastructure asset owners and operators in an effort to increase situational awareness, encourage discussion, and foster collaboration to help mitigate the risk of cyber attacks.

In 2006 the Group for Advanced Information Technology at the British Columbia Institute of Technology maintains a security incident tracking system known as the Industrial Security Incident Database (ISID). Their system records cybersecurity incidents that directly affect control systems, including accidental cyber-related incidents and deliberate external hacks, denial-of-service attacks, and virus/worm infiltrations. Figure B-4 summarizes the ISID statistics for the spring of 2006.

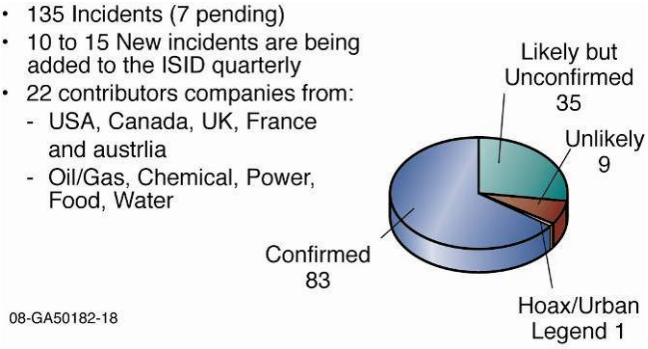


Figure B-4. Industrial ISID spring 2006 statistics.

Vulnerabilities have resulted in a number of security breaches.

Potential Consequences

Understanding the potential consequences of a cyber attack on a CIKR control system is essential for determining risk. Although these consequences have been limited in the United States thus far, DHS Secretary Chertoff recognized that: "The decentralized, asymmetrical nature of cyber threats makes them particularly dangerous. Not only is cybercrime expanding, but the potential damage is very much on a par with the 9/11/2001, attacks." According to the NIPP, the economic damages from the 9/11/2001 attacks alone were hundreds of billions of dollars.

Two examples show the potentially catastrophic consequences when control systems fail; though neither of these events involved a cyber attack, the attack evolution was similar to what could occur through malicious control of their control systems:

- The blackout that occurred on August 14, 2003, left 50 million people without power for 12 hours. This resulted in $10 billion in losses, based on disruptions to major industries and transportation infrastructures.[10]
- The BP Texas City Refinery accident in 2005 (see Figure B-5) resulted in 15 dead, 170 injured, and economic losses in excess of $1.5 billion.[11]

Figure B-5. BP refinery—Chemical Safety Board.

According to the NIPP, consequence is measured or calculated as the range of loss or damage that can be expected. These losses and damages can now be characterized in several different ways based on breadth of impact (single facility, sector wide, cascading/cross-sector) and type of impact (human, economic, public confidence, government capability). Each of these consequence categories is briefly discussed below.

Single Facility Events

Single facility events are mostly addressed in permitting and licensing processes and classified as normal routine accidents and incidents.

Sector Wide Events

Interdependencies within a sector, such as in the electrical or transportation sector, can cause a facility-specific incident to impact other facilities or points within the sector, amplifying the damage.

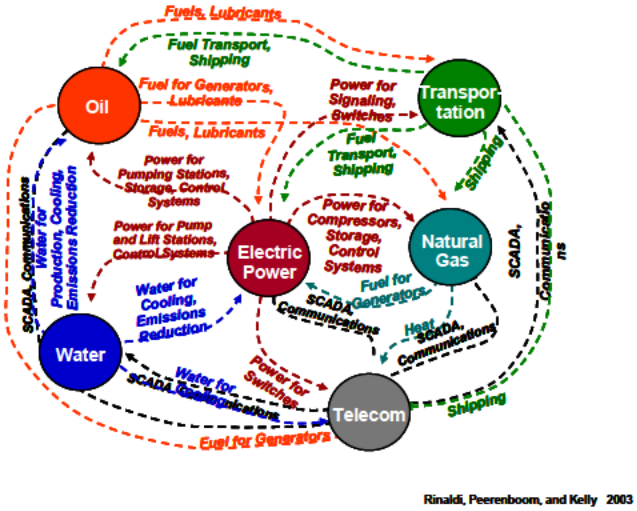
Cascading/Cross-Sector Events

Critical infrastructures are interdependent, interacting with each other through direct connections or the supply chain. An attack on one infrastructure could affect the direct operation of others or cause cascading health, safety, or economic impacts. These interactions, based on a flooding event and subsequent response, are illustrated in Figures B-6 and B-7.[12]

The following was taken from an INL report, *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research*.[13]

Interrelationships among infrastructures and the potential for cascading effects was never more evident than on July 19, 2001, when a 62-car freight train carrying hazardous chemicals derailed in Baltimore, Maryland. In addition to the expected effect on rail system traffic, automobile traffic, and emergency services, this disaster caused a cascading degradation of infrastructure components not previously anticipated.

Interstate 395, the baseball park, and the Inner Harbor were closed due to smoke (Figure B-8). The tunnel fire caused a water main to break above the tunnel (Figure B-9) shooting geysers 20 feet into the air and causing 3-foot-deep floods in some areas of the Howard Street Tunnel. The flooding knocked out electricity to 1,200 downtown Baltimore residences.[14] Fiber optic cables running through the tunnel were destroyed; resulting in major disruptions to telephone, email, Web, and data services. This affected major corporations, including WorldCom Inc., Verizon Communications Inc., the Hearst Corporation in New York City, Nextel Communications Inc., and the Baltimore Sun newspaper.[15] This event caused significant disruption to rail services across the Mid-Atlantic,[16] including delays in coal delivery and also limestone delivery for steel.



Rinaldi, Peerenboom, and Kelly 2003

Figure B-6. Interactions based on a flooding event and subsequent response.

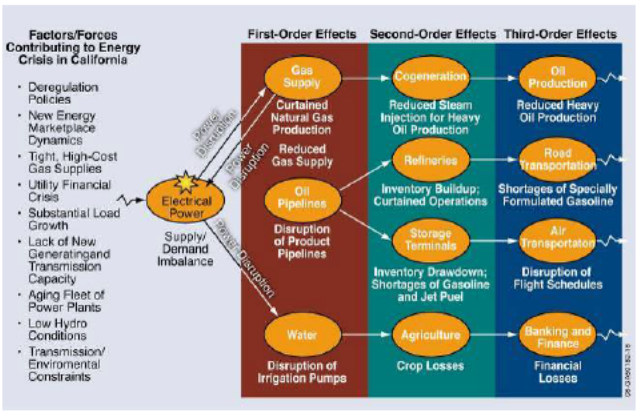


Figure B-7. Example of cascading consequence from the energy crisis.

Figure B-8. Thick, black smoke billows out of the railroad tunnel near Oriole Park at Camden Yards.

Figure B-9. An official surveys the gaping hole in a broken 40-inch water main at Howard and Lombard streets in Baltimore, Maryland.

Types of Impact

Based on the criteria set forth in HSPD-7 [Ref 4], the types of impacts being considered for the national-level comparative risk assessment are defined as:

- *Human*. The effect on human life and physical well-being (e.g., fatalities, injuries).
- *Economic*. Direct and indirect effects on the economy (e.g., cost to rebuild assets, cost to respond to and recover from attack, downstream costs, resulting from disruption of product or service, long-term costs due to environmental damage).
- *Government Capability*. A measure of the effect on the government's ability to maintain order, deliver minimum essential public services, ensure public health and safety, and carry out national security-related missions.
- *Public Confidence*. A measure of the effect on public morale and confidence in national economic and political institutions.

Current Status of Control System Security

One way to define the status of control systems security is to compare it to the state of IT security, there being many common issues. Table B-1 shows how these two systems compare on various major security topics. In all cases, control system security lags far behind the current state of IT security. It should be noted that the information in this table is not static. As awareness increases on threats and vulnerabilities, the evolution of control systems security is advancing.

The current status of control system security can also be defined based on recent assessment findings. These findings can be grouped into several key areas: general control systems, switches and routers, firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) as shown in Table B-2. Once again, these assessment results clearly show that there is considerable room for improvement.

Table B-1. Evolution of IT security vs. control system security (derived from PA Consulting Group).

Topic of Comparison	Information Technology	Control Systems
Anti-virus & Mobile Code Countermeasures	Common and widely used	Uncommon and difficult to deploy
Support Technology Lifetime	3 to 5 years	Up to 20 years
Outsourcing	Common and widely used	Rarely used
Application of Patches	Regular/scheduled	Slow (vendor specific)
Change Management	Regular/scheduled	Legacy based—unsuitable for modern security
Time Critical Content	Delays are usually accepted	Critical due to safety
Availability	Delays are usually accepted	24 × 7 × 365
Security Awareness	Good in both private and public sector	Generally poor regarding cybersecurity
Security Testing/Audit	Scheduled and mandated	Occasional testing for outages
Physical Security	Secure	Very good but often remote and unmanned

Table B-2. General findings.

Control Systems	Switches and Routers	Firewalls	IDS (passive)	IPS (active)
• Vendor default accounts and passwords • Guest accounts still available • Inappropriate use of enterprise services (DNS, NTP, www) • Inadequate security level agreements with both peer site and with vendors • Dynamic ARP tables with no ARP monitoring • Unused software still on systems • Unused services still active • Writeable shares between hosts • Direct VPN from offsite allowed to control systems	• Maintain state as was delivered: wide open • Limited onsite expertise to address security • In most cases, defaults are not shown in configuration lists • Port (process) security rarely used to secure domains	• Rules: - Many old and unused - Many without ownership or justification - Many not commented - Many generic or simplified • Logging not turned on • In some cases, firewall is subverted by direct connection • Same firewall rule set used on control domain as for the corporate domain	• New to control system environments - Only minimal set of signatures • Not always employed at corporate level • No budget or support for staffing and training for use in control domain • Cannot analyze encrypted traffic	• New to industry (in general) • Not fully understood in many applications • Difficult to employ at corporate level • No budget or support for staffing and training • Caution if deploying inside critical real-time system networks: - Packet scrubbing - False positives.

Barriers to Minimizing Risks

GAO Report 04-354 [Ref 3] assigned the significant challenges of securing control systems into three topical areas:

- Limitations of current security technologies in securing control systems
- Perception that securing control systems may not be economically justifiable
- Conflicting priorities within organizations regarding the security of control systems.

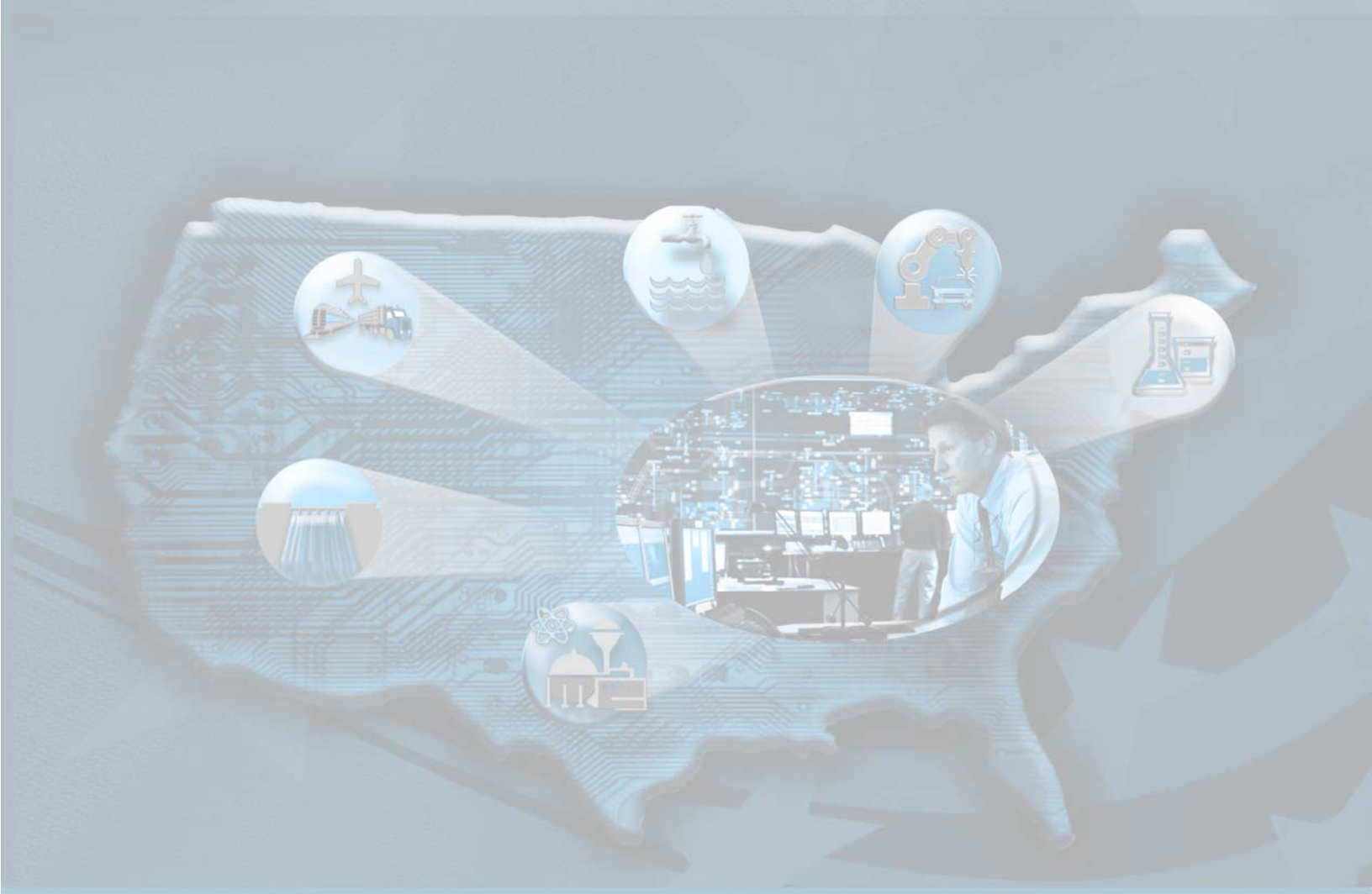
The text box on the right lists more specific technical and organizational barriers.

Technical and organizational barriers

- Inability to measure and assess security posture
- Lack of metrics and tools
- Competing business priorities
- Lack of business case
- Lack of threat information
- Reluctance to share information on control system incidents
- Division of security responsibilities
- Control Systems limited processing capabilities
- Control Systems design limitations
- Need for real-time operations
- Magnitude of the problem, so many infrastructures, so many control systems

REFERENCES

1. PDD/NSC-63, "Critical Infrastructure Protection," The White House, May 22, 1998, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.
2. *National Strategy to Secure Cyberspace*, The White House, February 2003, http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf.
3. GAO-04-354, "Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems," March 2004, http://www.gao.gov/new.items/d04354.pdf.
4. HSPD-7, "Critical Infrastructure Identification, Prioritization, and Protection," The White House, December 17, 2003, http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm.
5. *Remarks by Homeland Security Secretary Michael Chertoff to the 2008 RSA Conference, San Francisco, California, Moscone Center, RSA Conference*, Release Date: April 8, 2008, http://www.dhs.gov/xnews/speeches/sp_1208285512376.shtm.
6. Top Ten Vulnerabilities of Control Systems, September 7, 2004, http://www.nerc.com/docs/cip/Top_10_Vulnerabilities-mlp-7sep04.pdf.
7. US-CERT, Control Systems Security Program (CSSP), "Overview of Cyber Vulnerabilities," http://www.us-cert.gov/control_systems/csvuls.html.
8. US-CERT, "Technical Cyber Security Alerts," http://www.us-cert.gov/cas/techalerts/.
9. National Institute of Standards and Technology (NIST), "National Vulnerability Database," http://nvd.nist.gov/
10. Galvin Electricity Initiative, http://www.galvinpower.org/search.php?q=blackout%202003, visited June 6, 2008.
11. U.S. Chemical Safety and Hazard Investigation Board Investigation Report, Report No. 2005-04-I-TX, Refinery Explosion and Fire, March 2007, http://www.csb.gov/completed_investigations/docs/CSBFinalReportBP.pdf.
12. S. Rinaldi, J. Peerenboom, and T. Kelly. "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems Magazine*, IEEE, December 2001, pp.11-25.
13. Idaho National Laboratory, *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research*, INL/EXT-06-11464, August 2006.
14. L. Layton and D. Phillips, 2001, "Train Sets Tunnel Afire, Shuts Down Baltimore," Available online via < http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A17542-2001Jul18>, accessed March 28, 2002.
15. A. Ratner, July 20, 2001, "Train Derailment Severs Communications," Available online via http://www.baltimoresun.com/news/local/bal-email19,0,2261351.story?coll=bal-home-headlines, accessed June 3, 2008.
16. R. Little and P. Adams, 2001, "Tunnel Fire Choking East Coast Rail Freight," Available online via http://www.baltimoresun.com/news/local/bal-te.bz.freight20jul20,0,4829093.story, accessed June 3, 2008.



Appendix C

Public Private Coordination in Control Systems Security

This page intentionally left blank

Appendix C

Public Private Coordination in Control Systems Security

The following tables summarize the activities of 33 coordinating mechanisms dealing with control systems security.

1. Computer Emergency Readiness Team Coordination Center (CERT/CC)
2. FBI InfraGard
3. Federal Control Systems Security Working Group (Federal Partners)
4. Federal Plan for Cyber Security and Information Assurance Research and Development
5. Government Forum of Incident Response and Security Teams (GFIRST)
6. Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)
7. Information Sharing and Analysis Centers (ISACs)
8. Instrumentation, Systems, and Automation Society (ISA)
9. Interactive Energy Roadmap (ieRoadmap)
10. International Electrotechnical Commission (IEC)
11. Joint Terrorism Task Force (JTTF)
12. Law Enforcement Online (LEO)
13. Multi-State Information Sharing and Analysis Center (MS-ISAC)
14. National Cyber Response Coordination Group (NCRCG)
15. National Exercises—Cyber Storm
16. National Infrastructure Coordinating Center (NICC)
17. NIPP CIKR Protection Metrics Working Groups
18. Office of the Director of National Intelligence (ODNI)
19. Process Control Security Requirements Forum (PCSRF)
20. Standard Authorization Request
21. Technical Support Working Group (TSWG)
22. United States Computer Emergency Readiness Team (US-CERT)
23. Chemical Information Technology Center (ChemITC)

NIPP Partnership and CIPAC Groups:

24. Critical Infrastructure Partnership Advisory Council (CIPAC)
25. Cross Sector Cyber Security Working Group (CSCSWG)
26. Energy Sector Control Systems Working Group (ESCSWG)
27. Partnership for Critical Infrastructure Security (PCIS)
28. Process Control Systems Forum (PCSF) - Historical
29. Water Sector Coordinating Council Cyber Security Working Group (WSCC-CSWG)
30. Industrial Control Systems Joint Working Group (ICSJWG)

NIPP Processes and Mechanisms:

31. Homeland Security Information Network (HSIN)
32. NIPP Sector CIKR Protection Annual Report (SAR)/National CIKR Protection Annual Report (NAR)
33. NIPP Sector-Specific Plans (SSP)
34. National Plan for Research and Development in Support of Critical Infrastructure Protection (National R&D Plan)

1

Computer Emergency Readiness Team Coordination Center (CERT/CC)

Regional Coordination

Key Purpose: To identify and address existing and potential threats, notify system administrators and other technical personnel of these threats, and coordinate with vendors and incident response teams worldwide to address the threats.

Program Description: CERT/CC addresses risks at the software and system level. It analyzes vulnerabilities to identify and mitigate the issues before they become a significant security threat and works with the appropriate technology producers to resolve the issue. CERT/CC works to establish practices that vendors can use to improve the security and quality of their software. To promote a global response capability, CERT/CC helps organizations and countries establish computer security incident response teams (CSIRTs), and works with existing teams to coordinate communication and response during major security events. Its artifact analysts examine, catalog, and sometimes reverse-engineer malicious code.

Members and Key Partners:

Leadership: CERT

Website:
http://www.cert.org/certcc.html

Cross-cutting and Enabling Activities

- Assessments and analysis
- Outreach, awareness, and information sharing
- Vulnerabilities disclosure
- Threat information
- Incident reporting and situational awareness

2

FBI InfraGard

Regional Coordination

Key Purpose: To promote ongoing dialogue and timely communication between members and the FBI. InfraGard members gain access to information that enables them to protect their assets and in turn give information to government that facilitates its responsibilities to prevent and address terrorism and other crimes.

Program Description: InfraGard is a partnership between the FBI, other government entities, and the private sector. It is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants that enables the sharing of knowledge, expertise, information, and intelligence related to the protection of U.S. CIKR from physical and cyber threats. InfraGard Chapters are geographically linked with FBI Field Office territories. The InfraGard secure website provides members with information about recent intrusions, research related to critical infrastructure protection, and the capability to communicate securely with other members. It operates under the Other Information-Sharing Nodes. matters relevant to informed reporting of potential crimes and attacks on the nation and U.S. interests.

Members and Key Partners:

Members: FBI, state and local law enforcement, private businesses and academic institutions

Leadership: FBI Cyber Division

Federal: DHS, other federal organizations dealing with critical infrastructure protection

Website:
http://www.infragard.net/

Cross-cutting and Enabling Activities

- Training
- Recommended Practices
- Outreach, awareness, and information sharing
- Partnership development
- Vulnerabilities disclosure
- Threat information
- Interdependency issues
- Incident reporting and situational awareness

3

Federal Control Systems Security Working Group (Federal Partners)

National-Level Coordination

Key Purpose: To lead government coordination to secure critical infrastructure control systems.

Program Description: The Federal Partners comprises leaders from more than 30 Federal organizations with control systems security interests joining together to promote coordination among Federal agencies and encourage voluntarily information sharing about control systems activities. Since forming in 2006, the Federal Partners queried Federal agencies to find out the role they play in coordinating control systems security activities, and used that information to create the Federal Coordinating Strategy to Secure Control Systems: An Organizing Framework and Baseline of Federal Programs. This document outlined the vision, roles, and framework for Federal coordination. This document aided the creation of this Strategy.

Members and Key Partners:

Members: Leaders from Federal agencies dealing with control systems

Leadership: DHS NCSD

Cross-cutting and Enabling Activities

- Outreach, awareness, and information sharing
- Partnership development
- Interdependency issues

4

Federal Plan for Cyber Security and Information Assurance Research and Development

National-Level Coordination

Key Purpose: To provide baseline information and a coordinated interagency technical framework for addressing critical gaps in current cybersecurity and information assurance capabilities and technologies. It focuses on interagency R&D priorities and is intended to complement agency-specific prioritization and R&D planning efforts in cybersecurity and information assurance. The Plan also describes the key Federal role in supporting R&D to strengthen the overall security of the IT infrastructure through development of fundamentally more secure next-generation technologies.

Program Description: The Plan responds to calls for improved Federal cybersecurity and information assurance R&D from: the Office of Science and Technology Policy (OSTP)/Office of Management and Budget (OMB) Memorandum on Administration FY 2007 R&D Budget Priorities; *Cyber Security: A Crisis of Prioritization*, the 2005 report of the President's Information Technology Advisory Committee (PITAC); the 2003 *National Strategy to Secure Cyberspace*; and the 2002 Cyber Security Research and Development Act (P.L. 107-305). The Plan serves as a foundational document for the *National Critical Infrastructure Protection Research and Development Plan* (NCIP R&D Plan), which is required by HSPD-7.

The Plan was written and is being implemented by the Cyber Security and Information Assurance Interagency Working Group (CSIA IWG), which gathers information about agencies' cybersecurity and information assurance R&D programmatic activities.

Members and Key Partners:

Members: senior representatives from Federal agencies

Leadership: CSA IWG

Federal: CIA, DARPA, DOE, DHS, DOJ, Department of State, DOT, Department of the Treasury, Disruptive Technology Office, FAA, FBI, NASA, NIST, NIH, NSF, NSA, Office of the Secretary of Defense and Department of Defense Service research organizations, TSWG, U.S. Postal Service

Website:
http://www.nitrd.gov/pubs/csia/csia_federal_plan.pdf

Cross-cutting and Enabling Activities

- Research and development
- Assessments and analysis
- Recommended Practices
- Outreach, awareness, and information sharing
- Standards development
- Partnership development
- Vulnerabilities disclosure
- Threat information
- Metrics
- Interdependency issues

5

Government Forum of Incident Response and Security Teams (GFIRST)

National-Level Coordination

Key Purpose: To secure government information technology systems, handle computer security incidents, and encourage proactive and preventive security practices across government agencies. The GFIRST peer group provides members with technical information, tools, methods, assistance, and guidance; shares specific technical details regarding incidents within a trusted U.S. government environment on a peer-to-peer level; and works to improve incident response operations.

Program Description: GFIRST is a group of more than 50 technical and tactical practitioners from security response teams who promote cooperation among the full range of federal agencies, including defense, civilian, intelligence, and law enforcement. GFIRST, which operates under the United States Computer Emergency Readiness Team (US-CERT), contributes to SSPs under the NIPP. The GFIRST portal provides a secure, web-based collaborative system to share sensitive cyber-related information with participants in the public and private sector.

Members and Key Partners:

Members: U.S. citizens in a government cyber incident response team

Leadership: US-CERT and DHS

Federal: MS-ISAC, NCRCG, ISACS, CISO Forum

Website: http://www.us-cert.gov/federal/gfirst.html

Cross-cutting and Enabling Activities

- Research and development
- Training
- Recommended Practices
- Outreach, awareness, and information sharing
- Assessments and analysis
- Vulnerabilities disclosure
- Incident reporting and situational awareness

6

Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)

National-Level Coordination

Key Purpose: To bring together intelligence and infrastructure specialists to ensure a complete and sophisticated understanding of the risks to CIKR by integrating and analyzing intelligence and law enforcement information and owner/operator expertise on threats.

Program Description: HITRAC, formed in accordance with section 201 of the Homeland Security Act, develops analytical products by combining intelligence expertise based on all-source information, threat assessments, and trend analysis with practical business and CIKR operational expertise informed by current infrastructure status and operations information. This comprehensive analysis provides an understanding of the threat, CIKR vulnerabilities, the potential consequences of attacks, and the effects of risk-mitigation actions on not only the threat, but also on business and operations. This combination of intelligence and practical knowledge allows HITRAC to provide CIKR risk assessment products that contain strategically relevant and actionable information. It also allows HITRAC to identify intelligence collection requirements in conjunction with owners and operators so that the intelligence community can provide the type of information necessary to support the CIKR protection mission. Based on HITRAC analysis, DHS produces two classes of information that support the NIPP: information that supports responses to emergent threats or immediate incidents; and information that supports the strategic planning needed to enhance the protection of U.S. CIKR over the long term.

Members and Key Partners:

Federal: U.S. intelligence community, national law enforcement, GCCs

Others: SSAs, owners/operators, ISACs

Cross-cutting and Enabling Activities

- Research and development
- Assessments and analysis
- Outreach, awareness, and information sharing
- Standards development
- Law enforcement
- Partnership development
- Vulnerabilities disclosure
- Threat information
- Interdependency issues
- Business continuity
- Incident reporting and situational awareness

7

Information Sharing and Analysis Centers (ISACs)

Sector Partnership Coordination

Key Purpose: To advance physical and cyber CIKR protection efforts by establishing and maintaining frameworks for operational interaction between and among members and external security partners.

Program Description: Originally recommended by Presidential Decision Directive 63 (PDD-63) in 1998, ISACs are sector-specific entities that typically serve as the tactical and operational arms for sector information-sharing efforts. ISAC functions include, but are not limited to, supporting sector-specific information/intelligence requirements for incidents, threats, and vulnerabilities; providing secure capability for members to exchange and share information on cyber, physical, or other threats; establishing and maintaining operational-level dialogue with appropriate governmental agencies; identifying and disseminating knowledge and recommended practices; and promoting education and awareness.

Members and Key Partners:

Members: Public- and private-sector stakeholders

Federal: GCCs, SSAs,

Others: SCCs

Cross-cutting and Enabling Activities

- Recommended Practices
- Outreach, awareness, and information sharing
- Standards development
- Acquisition and Procurement
- Partnership development
- Vulnerabilities disclosure
- Threat information
- Interdependency issues
- Incident reporting and situational awareness

8

Instrumentation, Systems, and Automation Society (ISA)

National-Level Coordination

Key Purpose: To develop standards, certify industry professionals, provide education and training, publish books and technical articles, and host the largest conference and exhibition for automation professionals in the Western hemisphere.

Program Description: ISA is a global nonprofit organization that helps more than 30,000 worldwide members and other professionals solve difficult technical problems. ISA provides them with access to technical information, professional development resources, and opportunities to network with other automation professionals. A major ISA focus is the leadership and forum to establish international technical standards for the design and application of control systems. ISA has contributed to work with the National Institute of Standards and Technology (NIST), an agency of the U.S. Commerce Department's Technology Administration, as well as DHS efforts to reach out to various standards associations.

Members and Key Partners:

Members:

Leadership:

Federal:

Others:

Website: http://www.isa.org/

Cross-cutting and Enabling Activities

- Training
- Outreach, awareness, and information sharing
- Partnership development
- Standards development

9

Interactive Energy Roadmap (ieRoadmap)

National-Level Coordination

Key Purpose: To facilitate discovery of collaborative R&D opportunities, identify gaps in existing R&D, and measure progress in pursuing the strategies and goals established by the *Roadmap to Secure Control Systems in the Energy Sector*.

Program Description: This interactive website enables members of the energy sector's control systems community to map their R&D efforts to specific strategies and challenges identified by industry stakeholders in the Roadmap. The site is designed to provide up-to-date information on new and existing activities relevant to energy control systems security. The Roadmap is a groundbreaking strategy for protecting all energy control systems from intentional cyber assault within ten years. The ieRoadmap was created by DOE and the Energy Sector to aid in the implementation of the Roadmap's goals and priorities by allowing principal investigators of control systems security projects to post their projects and map their progress on a collaborative interactive forum.

Members and Key Partners:

Members: PIs of security projects

Federal: DOE, DHS

Others: PCSF

Website: http://www.controlsystemsroadmap.net/

Cross-cutting and Enabling Activities

- Research and development
- Assessments and analysis
- Outreach, awareness, and information sharing
- Partnership development
- Vulnerabilities disclosure
- Threat information
- Metrics
- Interdependency issues
- Incident reporting and situational awareness

10

International Electrotechnical Commission (IEC)

Regional Coordination

Key Purpose: To prepare and publish international standards for all electrical, electronic, and related technologies. These serve as a basis for national standardization and as references when drafting international tenders and contracts. Through its members, the IEC promotes international cooperation on all questions of electrotechnical standardization and related matters, such as the assessment of conformity to standards.

Program Description: The IEC was formed as a result of the Resolution of the Chamber of Government Delegates at the International Electrical Congress of St. Louis (U.S.A.), in September 1904.

The IEC works closely with its international standardization partners, the International Organization for Standardization (ISO) and the International Telecommunication Union (ITU), other regional standardization organizations and international organizations, including the World Health Organization (WHO), the International Labour Organization (ILO) and the United Nations Economic Commission for Europe (UNECE), the International Council on Large Electric Systems (CIGRE), the International Maritime Organization (IMO), the International Organization of Legal Metrology (OIML), the Union of the Electricity Industry (EURELECTRIC), the International Federation of Standards Users (IFAN), and the International Laboratory Accreditation Cooperation (ILAC).

Members and Key Partners:

Members: Manufacturers, providers, distributors and vendors, consumers and users, all levels of governmental agencies, professional societies and trade associations, standards developers

Website: http://www.IEC.ch

Cross-cutting and Enabling Activities

- Recommended Practices
- Outreach, awareness, and information sharing
- Standards development

11

Joint Terrorism Task Force

Regional Coordination

Key Purpose: To enhance communications, coordination, and cooperation among Federal, State, local, and tribal agencies representing the intelligence, law enforcement, defense, diplomatic, public safety, and homeland security communities by providing a point of fusion for terrorism intelligence and by supporting regional JTTFs throughout the United States.

Program Description: A JTTF is a partnership between the FBI, other federal agencies (notably Department of Homeland Security components), state and local law enforcement, and specialized agencies, such as railroad police that are charged with taking action against terrorism. JTTFs engage in surveillance, electronic monitoring, source development, and interviews in their pursuits. These operate under the Federal Intelligence Node of the NIPP and identify and establish the credibility of general and specific threats.

Members and Key Partners:

Members: Federal, state, and local law enforcement, FBI, specialized agencies dealing with terrorism

Website:
http://www.justice.gov/jttf/

Cross-cutting and Enabling Activities

- Assessments and analysis
- Training
- Recommended Practices
- Outreach, awareness, and information sharing
- Standards development
- Law enforcement
- Partnership development
- Threat information
- Interdependency issues
- Incident reporting and situational awareness

12

Law Enforcement Online (LEO)

National-Level Coordination

Key Purpose: To reduce terrorist and criminal activities by maximizing the ability to provide timely and relevant criminal justice information to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies concerning individuals, stolen property, criminal organizations and activities, and other law enforcement related data.

Program Description: LEO was established under the FBI Criminal Justice Information Services (CJIS) Division to provide a secure backbone network that members can use to store, process, and transmit Sensitive But Unclassified information. LEO members have access to a variety of services via LEO, including LEO Chat (an instant messaging service), eLearning for self-paced study, calendar services, e-mail, forums, special interest groups, and several crisis-management communication mechanisms. LEO operates under the NIPP Federal Intelligence Node.

Members and Key Partners:

Members: Law enforcement community, criminal justice officials, first responders, public safety officials, and members of the intelligence and counterintelligence communities

Leadership: Criminal Justice Information Services (CJIS)

Website:
http://www.fbi.gov/hq/cjisd/leo.htm

Cross-cutting and Enabling Activities

- Outreach, awareness, and information sharing
- Law enforcement
- Partnership development
- Vulnerabilities disclosure
- Threat information
- Incident reporting and situational awareness

13

Multi-State Information Sharing and Analysis Center (MS-ISAC)

Regional Coordination

Key Purpose: To provide a common mechanism for raising the level of cybersecurity readiness and response in each state and with local governments. The MS-ISAC provides a central resource for gathering information on cyber threats to critical infrastructure from the states and providing two-way sharing of information between and among the states and with local government.

Program Description: The MS-ISAC is a voluntary and collaborative organization with participation from all 50 states and the District of Columbia. The MS-ISAC goals are consistent with the objectives of the *National Strategy to Secure Cyberspace*, and these include: disseminating early warnings of cyber system threats; sharing security incident information; providing trending and other analysis for security planning; distributing current proven security practices and suggestions; and promoting awareness of the interdependencies between cyber and physical critical infrastructure, as well as between and among the different sectors.

The MS-ISAC Cyber and Spatial Analysis Center (CSAC) is a 24/7 operational center for the members. Vulnerabilities, threats and other significant cyber-related events are reported to the CSAC, which then distributes this information to members along with mitigation or protection information, if available.

Members and Key Partners:

Members: Cybersecurity programs from all 50 state governments and D.C.

Leadership: Nine-member executive committee

Federal: State and local governments

Website:
http://www.msisac.org/

Cross-cutting and Enabling Activities

- Recommended Practices
- Outreach, awareness, and information sharing
- Standards development
- Partnership development
- Vulnerabilities disclosure
- Threat information
- Interdependency issues
- Incident reporting and situational awareness

14

National Cyber Response Coordination Group (NCRCG)

National-Level Coordination

Key Purpose: To coordinate the Federal response, including US-CERT, law enforcement, and the intelligence community, in the event of a nationally significant cyber-related incident. The NCRCG provides subject-matter expertise related to the cyber threat, analysis, and recommendations in the event of a cyber-related Incident of National Significance.

Program Description: The NCRCG serves as the Federal government's principal interagency mechanism for coordinating the federal effort to respond to and recover from cyber incidents of national significance. During actual or potential Incidents of National Significance, the NCRCG coordinates with the Homeland Security Operations Center (HSOC) in disseminating critical information to and from government and non-government sources such as information-sharing mechanisms, academia, industry, and the public. The NCRCG was established through the Cyber Incident Annex of the National Response Plan. The NCRCG has developed concept of operations (CONOPS) for national cyber incident response that have been examined in the National Exercise Cyber Storm, conducted by NCSD with public and private sector stakeholders.

The NCRCG is also reviewing capabilities of federal agencies from a cyber defense perspective to better leverage and coordinate the preparation for and response to significant cyber incidents. NCRCG is a subset of the Interagency Incident Management Group which also includes US-CERT, the Intelligence Community – Incident Response Center (IC-IRC), and DOD.

Members and Key Partners:

Members: Senior representatives from 16 federal agencies

Leadership: DOD, DOJ, DHS/NCSD

Cross-cutting and Enabling Activities

- Assessments and analysis
- Recommended Practices
- Outreach, awareness, and information sharing
- Policy/regulation coordination and development
- Law enforcement
- Vulnerabilities disclosure
- Threat information
- Interdependency issues
- Business continuity
- Incident reporting and situational awareness

15

National Exercises—Cyber Storm

Sector Partnership Coordination

Key Purpose: To test communications, policies, and procedures in response to various cyber attacks and to identify where further planning and process improvements are needed.

Program Description: Cyber Storm, the Department of Homeland Security's biennial exercise series, provides the framework for the nation's largest cybersecurity exercise. Two successful exercises have been executed, one in February 2006 and one in March 2008. Congress mandated the Cyber Storm exercise series to strengthen cyber preparedness in the public and private sectors.

Cyber Storm II addresses the Training and Exercise requirements found in Homeland Security Presidential Directive 8 "National Preparedness." Coordinated under the DHS National Exercise Program, it supports the *National Strategy to Secure Cyberspace* by exercising the national cybersecurity response. It also exercises the standard operating procedures found in the draft Cyber Incident Annex of the *National Response Framework*.

The exercises simulated a sophisticated cyber attack campaign through a series of scenarios directed at several critical infrastructure sectors. The intent of these scenarios was to highlight the interconnectedness of cyber systems with physical infrastructure and to exercise coordination and communication between the public and private sectors.

Members and Key Partners:

Leadership: DHS NCSD, DHS National Exercises Program

Federal: ISACs, GCCs, federal, state, local, and international governments

Others: SCCs, private sector

Website: http://www.dhs.gov/xprepresp/training/gc_1204738275985.shtm

Cross-cutting and Enabling Activities

- Training
- Recommended Practices
- Outreach, awareness, and information sharing
- Partnership development
- Threat information
- Interdependency issues
- Business continuity
- Incident reporting and situational awareness

16

National Infrastructure Coordinating Center (NICC)

National-Level Coordination

Key Purpose: To provide a centralized mechanism and process for information sharing and coordination between the government, SCCs, GCCs, and other industry partners, as well as disseminate products originated by HITRAC that contain all-hazards warning, threat, and CIKR protection information.

Program Description: The NICC is a 24/7 watch/operations center that maintains ongoing operational and situational awareness of the nation's CIKR sectors. The NICC receives situational, operational, and incident information from the CIKR sectors, in accordance with information-sharing protocols established in the NRP. The NICC is part of the DHS Office of Infrastructure Protection and is one of five designated elements of the DHS National Operations Center.

Members and Key Partners:

Federal: DHS, National Response Coordination Center (NRCC)

Cross-cutting and Enabling Activities

- Outreach, awareness, and information sharing
- Vulnerabilities disclosure
- Threat information
- Incident reporting and situational awareness

17

NIPP CIKR Protection Metrics Working Group

Sector Partnership Coordination

Key Purpose: To provide an opportunity and a forum for facilitating the development and implementation of metrics that can be used to measure the efficacy of risk management activities performed under the NIPP and the progress made in managing the risks of the nation's CIKR to terrorist attack and other hazards so as to inform national and sector-level risk management decisions.

Program Description: SSAs and other Federal departments and agencies with special functions related to CIKR, as designated in Homeland Security Presidential Directive 7 (HSPD-7), work in partnership with the Department of Homeland Security (DHS) to address the four principal NIPP CIKR Protection Metrics components: CIKR Protection Core Metrics; CIKR Protection Programmatic Metrics; Sector Partnership Metrics; and Sector-Specific Performance Metrics.

Core Metrics help measure progress in SSP implementation. Protection Programmatic Metrics are developed on the basis of requirements set out in the NIPP and supplemented by the activities called out in the National Annual Report and individual SSPs, and are intended to ensure that needed programs, products, and tools are developed to support NIPP- and SSP-related activities. Sector Partnership Metrics provide a point of reference for individual CIKR sectors to reflect their distinctive characteristics and requirements. Sector-Specific Performance Metrics contribute to the NIPP goal by addressing the specific protection challenges the sector faces and their distinct business continuity needs. This working group operates under the NIPP Federal Infrastructure Node.

Members and Key Partners:

Members: Representatives from SSAs and DHS OIP

Leadership: DHS OIP

Federal: GCCs, Federal agencies related to CIKR protection

Cross-cutting and Enabling Activities

- Recommended Practices
- Outreach, awareness, and information sharing
- Policy/regulation coordination and development
- Law enforcement
- Partnership development
- Vulnerabilities disclosure
- Threat information
- Metrics
- Interdependency issues
- Business continuity
- Incident reporting and situational awareness

18

Office of the Director of National Intelligence (ODNI)

National-Level Coordination

Key Purpose: To collect, analyze, and disseminate accurate, timely, and objective intelligence to the president and all who make and implement U.S. national security policy. The office conducts the U.S. Government's national intelligence program, deploys effective counterintelligence measures, and integrates foreign, military, and domestic intelligence in defense of the homeland and of U.S. interests abroad.

Program Description: The ODNI performs duties as outlined in the Intelligence Reform and Terrorist Prevention Act (IRTPA) of 2004, including ensuring accurate collection and analysis of national intelligence and overseeing coordination of relationships with foreign governments and international organizations. The office released in 2008 the *United States Intelligence Community Information Sharing Strategy*, which outlines a vision for an integrated intelligence enterprise that anticipates mission needs for information by making the complete spectrum of intelligence information seamlessly available to support all stages of the intelligence process. This document lays out a strategy to establish this new culture and to share information better.

The ODNI releases threat advisory information to the control systems community in its efforts to share information that will help secure cyberspace against attack. It operates under the Federal Intelligence node of the NIPP.

Members and Key Partners:

Leadership: The president, the National Security Council, and the Homeland Security Council

Federal: policymakers, military, the intelligence community

Website: http://www.dni.gov/

Cross-cutting and Enabling Activities

- Assessments and analysis
- Outreach, awareness, and information sharing
- Threat information

19

Process Control Security Requirements Forum (PCSRF)

Sector Partnership Coordination

Key Purpose: To increase the security of industrial process control systems through the definition and application of a common set of information security requirements for these systems. This will reduce the likelihood of successful cyber-attack on the nation's critical infrastructures.

Program Description: The PCSRF has more than 600 members from the government, academia, and private sectors, representing critical infrastructures and related process industries including oil and gas, water, electric power, chemicals, pharmaceuticals, metals and mining, and pulp and paper. Led by NIST, the PCSRF is a working group of users, vendors, and integrators in the process control industry aiming to present a cohesive, cross-industry, baseline set of security requirements for new industrial control systems.

NIST is working to improve the IT security of networked digital control systems used in industrial applications and created the PCSRF to address security requirements of process control systems.

Members and Key Partners:

Members: More than 600 international representatives of government and private sectors

Leadership: NIST

Federal: US-CERT CSSC, I3P, TSWG, etc.

Others: EPRI, NERC, ISA, etc.

Website: http://www.isd.mel.nist.gov/projects/processcontrol/

Cross-cutting and Enabling Activities

- Recommended Practices
- Outreach, awareness, and information sharing
- Standards development
- Policy/regulation coordination and development

20

Standard Authorization Request (SAR)

Regional Coordination

Key Purpose: A form to request urgent action, a new standard, revision to an existing standard, or withdrawal of an existing standard as the standard pertains to cybersecurity.

Program Description: The SAR is a form used by the North American Electric Reliability Corporation (NERC). NERC adopted Cyber Security Standards CIP-002-009 in 2006 and they were approved by the Federal Energy Regulatory Commission (FERC); eight standards became mandatory on January 17, 2008. The standards establish the minimum requirements needed t ensure the security of electronic exchange of information needed to support the reliability and the bulk power system. The SAR and NERC standards complement the NIPP in its protection of CIKR, specifically in the energy sector.

Members and Key Partners:

Leadership: NERC

Others: Standards users

Website: http://www.nerc.com/docs/standards/sar/MOD-030_Revisions_SAR_45-day_Comment_12Aug08.pdf

Cross-cutting and Enabling Activities

- Standards development

21

Technical Support Working Group (TSWG)

National-Level Coordination

Key Purpose: To identify, prioritize, and execute research and development, testing, evaluation, and commercialization efforts that satisfy interagency requirements for security technology to protect personnel, vital equipment, and facilities against terrorist attacks (mission of Infrastructure Protection focus area).

Program Description: TSWG is the national interagency research and development program for combating terrorism requirements at home and abroad, and cybersecurity activities are carried out by the Infrastructure Protection focus area within the Physical Security subgroup. Infrastructure Protection sponsors projects that develop technological solutions for the protection and assurance of defense-critical infrastructure systems vital to national and economic security. Technologies include those to (1) prevent and mitigate threats to computer networks and (2) standardize methodologies and decision aids for the analysis of elements to secure the nation's infrastructure, including power generation, utilities transmission, water supplies, and health services.

TSWG operates under the Department of State and the Department of Defense. Infrastructure protection activities contribute to responsibilities of DOD, DHS, and other agencies per HSPD-7. TSWG is a contributor to "Federal Plan for Cyber Security and Information Assurance Research and Development," developed by Cyber Security and Information Assurance Interagency Working Group (CSIA IWG).

Members and Key Partners:

Members: Senior representatives from lead and federal partner agencies

Leadership: DOD, Department of State

Federal: DHS S&T, DHS NCSD, DOE, FBI, CIA

Others: AGA, BCIT, first responders and other representatives from state and local governments as well as international agencies

Website: http://www.tswg.gov

Cross-cutting and Enabling Activities

- Research and development
- Assessments and analysis
- Recommended Practices
- Outreach, awareness, and information sharing
- Threat information
- Incident reporting and situational awareness

22

U.S. Computer Emergency Readiness Team (US-CERT)

National-Level Coordination

Key Purpose: To coordinate defense against and response to cyber attacks; to analyze and reduce cyber threats and vulnerabilities; to disseminate cyber threat warning information; and to coordinate incident response activities.

Program Description: US-CERT is the operational arm of the DHS National Cyber Security Division (NCSD). It is a public-private partnership whose activities include assessing and managing control system vulnerabilities, assisting the US-CERT Control Systems Security Center with control system incident management, and providing control system situational awareness through outreach and training initiatives.
The NCSD was established by DHS to serve as the federal government's cornerstone for cybersecurity coordination and preparedness, including implementation of the National Strategy to Secure Cyberspace. As US-CERT grows, it will include partnerships with private sector cybersecurity vendors, academia, federal agencies, Information Sharing and Analysis Centers (ISACs), state and local governments, and domestic and international organizations. Working together, these groups will coordinate national and international efforts to address key cybersecurity issues.

Members and Key Partners:

Members:

Leadership: DHS NCSD

Federal: DHS, Federal agencies

Others: industry, the research community, state and local governments

Website: http://www.us-cert.gov/aboutus.html#events

Cross-cutting and Enabling Activities

- Assessments and analysis
- Outreach, awareness, and information sharing
- Vulnerabilities disclosure
- Threat information
- Incident reporting and situational awareness

NIPP Partnership and CIPAC Groups

23

Chemical Information Technology Center (ChemITC)

Sector Partnership Coordination

Key Purpose: To address common information technology (IT) issues and support the industry's ability to safely and efficiently deliver products essential to society.

Program Description: ChemITC, part of the American Chemistry Council (ACC), is a forum for companies in and associated with the ACC to address common IT issues together, through a number of strategic programs.

The Chemical Sector Cyber Security Program focuses on risk management and reduction to minimize the potential impact of cyber attacks on business and manufacturing systems. The program coordinates with DHS on cybersecurity activities, provides members a place to network and share information, and offers members guidance documents through white papers and webcasts.

Industry Networking Groups give members a forum for conversation and coordination on IT activities. The Survey and Benchmarking Program queries ChemITC members on their use of IT, providing chemical company IT executives with a better understanding of common industry wide practices and trends and helps them make more informed IT decisions in the future.

Members and Key Partners:

Members: Public-sector cybersecurity leaders and industry organizations

Federal: DHS

Website:
http://www.chemitc.com

Cross-cutting and Enabling Activities

- Research and development
- Recommended Practices
- Outreach, awareness, and information sharing
- Partnership development
- Vulnerabilities disclosure
- Threat information
- Business continuity

24

Critical Infrastructure Partnership Advisory Council (CIPAC)

Sector Partnership Coordination

Key Purpose: To support implementation of the NIPP and help to effectuate the sector partnership model set forth in the NIPP by coordinating Federal infrastructure protection programs with the infrastructure protection activities of the private sector and of State, local, territorial, and tribal governments.

Program Description: The CIPAC represents a partnership between government and critical infrastructure/key resource (CIKR) owners and operators and provides a forum in which they can engage in a broad spectrum of activities to support and coordinate critical infrastructure protection, including: planning, coordination, security program implementation, operational activities related to critical infrastructure protection security measures, and information sharing about threats, vulnerabilities, protective measures, recommended practices, and lessons learned. The CIPAC was created under section 201 of the Homeland Security Act of 2002.

Members and Key Partners:

Members: SCC and GCC members

Website: http://www.dhs.gov/xprevprot/committees/editorial_0843.shtm

Cross-cutting and Enabling Activities

- Recommended Practices
- Outreach, awareness, and information sharing
- Policy/regulation coordination and development
- Partnership development
- Vulnerabilities disclosure
- Threat information
- Interdependency issues
- Business continuity
- Incident reporting and situational awareness

25

Cross Sector Cyber Security Working Group (CSCSWG)

National-Level Coordination

Key Purpose: To address cross sector cyber risk and explore interdependencies. The working group serves as a forum to bring government and the private sector together to address common cybersecurity elements and opportunities across the 17 critical infrastructure and key resource sectors.

Program Description: The CSCSWG, will provide the formal organizational structure for vetting and validating elements of a national strategy for coordination, done by the DHS National Cyber Security Division. The group will provide keen sector insights on where control systems can have major effects and consequences given successful attack on that infrastructure.

The CSCSWG was established under the auspices of the Critical Infrastructure Partnership Advisory Council (CIPAC).

Members and Key Partners:

Members: industry experts

Leadership: IT, DHS, Energy sector

Federal: DHS NCSD

Cross-cutting and Enabling Activities

- Recommended Practices
- Outreach, awareness, and information sharing
- Policy/regulation coordination and development
- Partnership development
- Interdependency issues

26

Energy Sector Control Systems Working Group (ESCSWG)

Sector Partnership Coordination

Key Purpose: To help guide implementation of the priorities identified in the industry-led *Roadmap to Secure Control Systems in the Energy Sector*. The group seeks to provide a platform for pursuing innovative and practical activities that will improve the cybersecurity of the control systems that manage our nation's energy infrastructure.

Program Description: The ESCSWG is a unique public-private partnership made up of representatives from the Government Coordinating Council for Energy, the Electric Sector Coordinating Council, and the Oil & Natural Gas Sector Coordinating Council. It operates under the framework of the Critical Infrastructure Partnership Advisory Council, a group formed under the National Infrastructure Protection Plan to support the private sector and government in collaborating on infrastructure protection activities.

Members and Key Partners:

Members: Representatives from energy SCCs and GCCs

Federal: DOE

Others: private sector stakeholders

Cross-cutting and Enabling Activities

- Assessments and analysis
- Recommended Practices
- Outreach, awareness, and information sharing
- Policy/regulation coordination and development
- Partnership development
- Vulnerabilities disclosure
- Threat information
- Metrics
- Interdependency issues

27

Partnership for Critical Infrastructure Security (PCIS)

National-Level Coordination

Key Purpose: To coordinate cross-sector initiatives that promote public and private efforts to help ensure secure, safe, and reliable critical infrastructure services.

Program Description: PCIS addresses cross-sector critical infrastructure protection and interdependency issues of concern to critical infrastructure owners and operators. In 2006, the National Infrastructure Protection Plan (DHS 2006) recognized the PCIS as the Private Sector Cross-Sector Council within the sector partnership framework as recommended by the National Infrastructure Advisory Council (NIAC 2005). In this role, the PCIS works with the Government Cross-Sector Council to collaborate on high-level critical infrastructure issues. PCIS develops cross-sector policy, strategy, and interdependency issues affecting the critical infrastructure sectors.

The PCIS provides a forum to share SSPs and for representatives of the SCCs to address important cross-sector issues and coordinate the needs of owners and operators in the sector partnership framework. The PCIS coordinates with the NIAC as needed on the security of the critical infrastructure sectors and their information systems. The PCIS also coordinates with the ISAC Council on communication issues related to threat indications, vulnerabilities, and protective strategies. The PCIS uses HSIN to enable sectors to share information with other sectors as appropriate.

Members and Key Partners:

Members: 17 SCC chairpersons

Website: http://www.pcis.org

Cross-cutting and Enabling Activities

- Recommended practices and training
- Outreach, awareness, and information sharing
- Policy/regulation coordination and development
- Partnership development
- Threat information
- Metrics
- Interdependency issues
- Business continuity
- Incident reporting and situational awareness
- Cross-sector strategies

28

Process Control Systems Forum (PCSF) (Historical)

National-Level Coordination

Key Purpose: Previously organized to facilitate the collaboration of control systems stakeholders to accelerate the design, development, and deployment of more secure control and legacy control systems. This organization was dissolved and replaced by the Industrial Control Systems Joint Working Group (ICSJWG).

Program Description: The PCSF was an initial effort to develop a collaborative, voluntary forum designed to leverage and unify the experience, capabilities, and contributions of international stakeholders from government, academia, industry users, owner/operators, systems integrators, and the vendor community through meetings, interest groups, and working groups, to develop and adopt common architectures, protocols, and practices.

Many of the PCSF coordinating and collaborative functionality will be replaced under a CIPAC Industrial Control Systems Joint Working Group. This ICSJWG supports the CSSP mission to focus collaborative efforts of public, private, and international entities to secure control systems cyberspace in support of the National Infrastructure Protection Plan. Participants address efforts of mutual interest within various stakeholder communities, build upon existing efforts, reduce redundancies, and contribute to national and international security efforts.

Members and Key Partners:

Former Members: international control systems stakeholders

Cross-cutting and Enabling Activities

- Recommended Practices
- Outreach, awareness, and information sharing
- Standards development
- Policy/regulation coordination and development
- Partnership development
- Interdependency issues

29

Water Sector Coordinating Council Cyber Security Working Group (WSCC-CSWG)

Sector Partnership Coordination

Key Purpose: The WSCC serves as a policy, strategy, and coordination mechanism and recommends actions to reduce and eliminate significant homeland security vulnerabilities to the water sector through interactions with the federal government and other critical infrastructure sectors. The CSWG is an integral part of these efforts.

Program Description: The WSCC-CSWG is an organization of 32 control systems security experts representing 29 drinking water and wastewater utilities, three industry associations, and one government agency. In March of 2008, the WSCC-CSWG released the Roadmap to Secure Control Systems in the Water Sector, an industry-led effort to create a sound R&D path for reducing the cyber risk of control systems used in the nation's water infrastructure. It established a vision that in 10 years, industrial control systems for critical applications will be designed, installed, and maintained to operate with no loss of critical function during and after a cyber event.

The National Infrastructure Protection Plan calls for private sector coordinating councils (SCCs) in each sector representing the nation's critical infrastructures. The CSWG is an integral part of the WSCC.

Members and Key Partners:

Members: AWWA, AMWA, experts from water utilities, industry associations, and the government

Federal: EPA, DHS, Water GCC

Others: PCIS

Cross-cutting and Enabling Activities

- Research and development
- Assessments and analysis
- Training
- Recommended Practices
- Outreach, awareness, and information sharing
- Policy/regulation coordination and development
- Partnership development
- Vulnerabilities disclosure
- Threat information
- Interdependency issues
- Business continuity
- Incident reporting and situational awareness

30

Industrial Control Systems Joint Working Group (ICSJWG)

National-Level Coordination

Key Purpose: The purpose of the Industrial Control Systems Joint Working Group (ICSJWG) is to facilitate the collaboration of control systems stakeholders to accelerate the design, development, and deployment of more secure control systems.

Program Description: The Industrial Control Systems Joint Working Group is a collaborative and coordination body operating under CIPAC regulations. Participants include international stakeholders, government, academia, owner/operators, system integrators, and the vendor community. The Industrial Control Systems Joint Working Group is sponsored by The Department of Homeland Security (DHS) National Cyber Security Division (NCSD) Control System Security Program (CSSP). The ICSJWG supports CSSP's mission to guide and coordinate the efforts of public, private, and international entities to reduce cyber security risks to control systems.

Members and Key Partners:

Govvernment Coordinating Council; Sector Coordinating Council; ICS subject matter experts

Cross-cutting and Enabling Activities

- Subgroups to develop specific products and deliverables
- Outreach, awareness, and information sharing
- Contr bute to national and international security efforts
- Cross-sector coordination of ICS security initiatives
- Control system specific issues and challenges
- Interdependency issues

NIPP Processes and Mechanisms

31

Homeland Security Information Network (HSIN)

Regional Coordination

Key Purpose: To enable real-time sharing of threat information to aid in combating terrorism, provide situational awareness, and provide advanced analytic capabilities.

Program Description: HSIN is a national, Web-based communications platform that allows DHS; SSAs; state, local, tribal, and territorial government entities; 50 major urban areas; and other security partners to obtain, analyze, and share information based on a common operating picture of strategic risk and the evolving incident landscape. This allows real-time interaction with the National Operations Center.

The network is designed to support both NIPP-related steady-state CIKR protection and NRP-related incident management activities, and to provide the information-sharing processes that form the bridge between these two homeland security missions. All NIPP nodes feed into and use this network. HSIN will be one part of the information-sharing environment (ISE) called for by the Intelligence Reform and Terrorism Prevention Act of 2004; as specified in the act, it will provide users with access to terrorism information that is matched to their roles, responsibilities, and missions in a timely and responsive manner.

The HSIN for Critical Sectors (HSIN-CS) is a collection of portals established to support and encourage information sharing in the critical infrastructure community of interest (COI).

Members and Key Partners:

Members: DHS; SSAs; State, local and tribal government entities; and other security partners

Cross-cutting and Enabling Activities

- Assessments and analysis
- Outreach, awareness, and information sharing
- Partnership development
- Threat information
- Incident reporting and situational awareness

32

NIPP Sector CIKR Protection Annual Report (SAR)/National CIKR Protection Annual Report (NAR)

National-Level Coordination

Key Purpose: To report information on sector-specific protection priorities, requirements, and resource needs; this information informs the NAR, which develops national priorities, identifies gaps or shortfalls, and supports strategic and investment decisions.

Program Description: HSPD-7 requires SSAs to provide an annual report to the Secretary of Homeland Security on their efforts to identify, prioritize, and coordinate CIKR protection in their respective sectors. Consistent with this requirement, DHS provides reporting guidance and templates that include requests for specific information, such as sector CIKR protection priorities, requirements, and resource needs.

DHS uses the SARs to inform the NAR, which analyzes information about sector priorities, requirements, and programs in the context of the National Risk Profile, a high-level summary of the aggregate risk and protective status of all sectors. The National Risk Profile drives the development of national priorities, which, in turn, are used to assess existing CIKR programs and to identify existing gaps or shortfalls in national CIKR protection efforts. This analysis provides the Executive Office of the President with information that supports both strategic and investment decisions related to CIKR protection.

The SARs provide a common vehicle for communicating CIKR protection performance and progress, and establish a baseline of existing sector-specific CIKR protection priorities, programs, and initiatives against which future improvements will be assessed.

Members and Key Partners:

Federal: DHS, SSAs, GCCs

Others: SSAs

Cross-cutting and Enabling Activities

- Outreach, awareness, and information sharing
- Policy/regulation coordination and development
- Threat information
- Interdependency issues

33

NIPP Sector-Specific Plans (SSPs)

National-Level Coordination

Key Purpose: To provide the means by which the NIPP is implemented across all critical infrastructure and key resources sectors, as well as a national framework for each sector to address its unique characteristics and risk landscape.

Program Description: Based on guidance from DHS, SSPs are developed jointly by SSAs in close collaboration with SCCs, GCCs, and others, including state, local, and tribal homeland security partners with key interests or expertise appropriate to the sector.

SSPs support the NIPP by establishing a coordinated approach to national priorities, goals, and requirements for critical infrastructure and key resources protection. The SSPs are an integral component of the NIPP and exist as independent documents to address the unique perspective, risk landscape, and methodologies associated with each sector. Each SSP will be continuously reviewed and regularly updated, improved, and modified as appropriate. SSPs operate in both federal infrastructure and private sector nodes, as it encourages and allows for collaboration between each.

Members and Key Partners:

Members: SSAs

Leadership: DHS and sector leaders

Federal: GCCs

Others: SCCs

Website:
http://www.dhs.gov/xprevprot/programs/gc_1179866197607.shtm

Cross-cutting and Enabling Activities

- Recommended Practices
- Outreach, awareness, and information sharing
- Policy/regulation coordination and development
- Partnership development
- Interdependency issues

34

National Plan for Research and Development in Support of Critical Infrastructure Protection

National-Level Coordination

Key Purpose: To create a plan, updated annually, that identifies major research and technology development efforts within federal agencies and articulates a vision that takes into account future needs and identifies research gaps based on known threats. The Plan has three strategic goals: a national common operating picture for critical infrastructure; a next-generation computing and communications network with security "designed-in" and inherent in all elements; and a resilient, self-diagnosing, and self-healing physical and cyber infrastructure systems.

Program Description: Homeland Security Presidential Directive #7 (HSPD-7) mandates that an annual Federal Critical Infrastructure Protection R&D Plan be developed by the White House Office of Science and Technology Policy (OSTP) and the Department of Homeland Security (DHS). The National Science and Technology Council (NSTC) infrastructure subcommittee develops the plan with support from two interagency working groups, Physical Structures and Systems and Critical Information Infrastructure Protection. The Plan was developed in close coordination with the National Infrastructure Protection Plan.

Members and Key Partners:

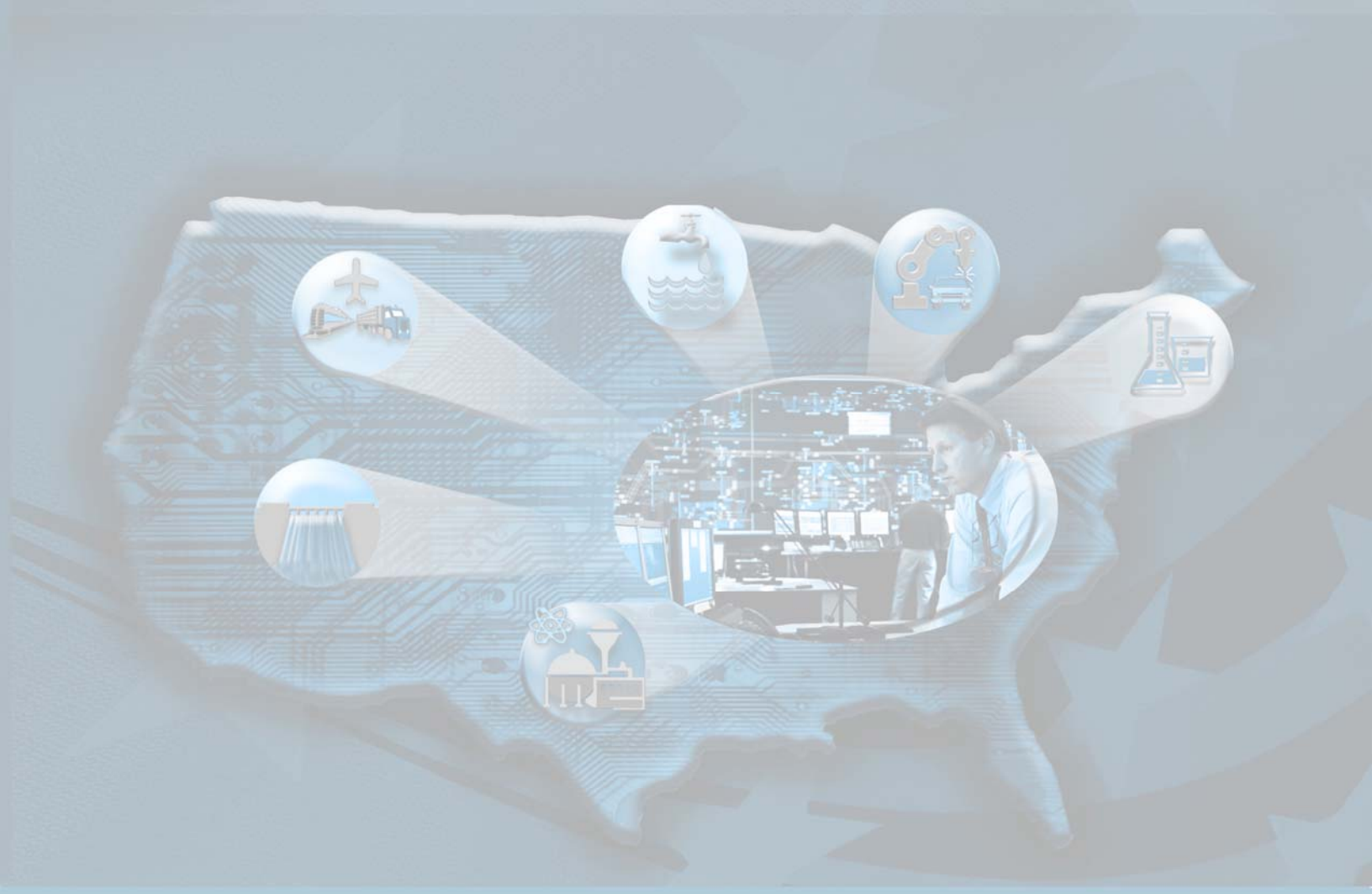
Leadership: OSTP and DHS S&T

Federal: All critical infrastructure sectors

Website:
http://www.dhs.gov/xlibrary/assets/ST_2004_NCIP_RD_PlanFINALApr05.pdf

Cross-cutting and Enabling Activities

- Research and development
- Recommended Practices
- Outreach, awareness, and information sharing
- Partnership development



Appendix D
Private Sector Organizations/Programs Control Systems Security Activities

This page intentionally left blank

Appendix D

Private Sector Organizations/Programs Control Systems Security Activities

The following table provides summary descriptions of industry, trade, professional and state organizations or programs that provide opportunities for coordination within CIKR that have interest or current activities within control systems security.

Table D-1. Description of private sector program cybersecurity activities.

Sector	Program/Organization	Description	Activity
Energy (Electric)	(IEEE) Institute of Electrical and Electronics Engineers, Inc.	As a nonprofit organization, IEEE is the world's leading professional association for the advancement of technology.	Since 1980, the IEEE Symposium on Security and Privacy has been the premier forum for the presentation of developments in computer security and electronic privacy, and for bringing researchers and practitioners in the field together. Papers offer novel research contributions in any aspect of computer security or electronic privacy. Papers may represent advances in the theory, design, implementation, analysis, or empirical evaluation of secure systems, either for general use or for specific application domains. The Institute of IEEE-USA supports increased funding for cybersecurity research and encourages developing programs for cybersecurity commercialization and workforce education, as well as programs to ensure the security of our cyber network systems, software, and personnel. To enhance the protection of our cybersecurity resources against a potential, concerted terrorist attack, IEEE-USA further recommends that Congress and the executive branch work in conjunction with private industry to authorize and appropriate increased and stable funding for cybersecurity research. The basic research foundation should be dramatically expanded within programs at the Defense Advanced Research Projects Agency, Department of Homeland Security-Homeland Security Advances Research Projects Agency, National Science Foundation, Department of Energy, the armed forces services, (Air Force Office of Scientific Research, Office of Naval Research, Army Research Office), Department of Health and Human services, including Public Health, Centers for Disease Control (CDC), the developing National Health Information Infrastructure, and the intelligence community. The government should continue to: • Encourage and enhance cross-agency and multidisciplinary collaboration, and improved techniques and processes, coordinating efforts between R&D labs, industry, academia, and the government • Encourage and promote industry's rapid transfer of basic and applied research results to technology and product development • Promote collaboration among federal laboratories, universities, and industry to foster an environment for rapid application of new cybersecurity solutions • Work with industry to facilitate the timely commercialization of cybersecurity advances from research laboratories to the marketplace • Work with industry and standards organizations such as American National Standards Institute, International Organization for Standardization and the IEEE to facilitate the establishment of international standards to help industry institute baselines of acceptable security for cyber systems • Encourage and financially support developing curricula and instruction for more effective teaching and training in cybersecurity at all educational levels. IEEE promotes security of all types of communication networks and forms of information transported by them and through them, end-to-end. Its security interests start from the network physical layer and end on the end user application layer. The committee support conferences, symposia, technical sessions, publications, etc., where information is exchanged within the scope of interest of the TC.

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
Energy (Electric) continued	International Electrotechnical Commission (IEC)	IEC prepares and publishes international standards for all electrical, electronic, and related technologies.	IEC has approximately 121 TC/SC organizations and liaisons internationally. They are involved in: • meeting the requirements of the global market efficiently • ensuring primacy and maximum worldwide use of its standards and conformity assessment schemes • assessing and improve the quality of products and services covered by its standards • establishing the conditions for the interoperability of complex systems • increasing the efficiency of industrial processes • contributing to the improvement of human health and safety • contributing to the protection of the environment.
	International Council on Large Electric Systems (CIGRE)	CIGRE is one of the leading worldwide organizations on electric power systems, covering their technical, economic, environmental, organizational, and regulatory aspects.	CIGRE develops technical knowledge using conferences and meetings to produce and discuss papers, and continuously work on technical subjects, conducted by its permanent study committees. Individual members are in the engineering, teaching, and research professions as well as other professions involved in the Industry (lawyers, economists, regulators…). Collective members consist of public or private companies of industrial and/or commercial character scientific or technical organizations, research institutes, and educational and administrative bodies.
Energy (Petroleum)	American Petroleum Institute (API)	API represents all aspects of America's oil and natural gas industry. It has 400 corporate members from all segments of the industry consisting of producers, refiners, suppliers, pipeline operators and marine transporters, and service and supply companies that support all industry segments.	API provides a forum where industry can come together and discuss important issues with government, develop industry guidelines, and share recommended practices. Members of API are committed in taking a leadership role in developing industry safe operating practices, assessing vulnerability at facilities, and coordinating emergency response training to ensure the safety and security of workers and surrounding communities and provide the transparent flow of reliable energy Americans have come to expect in their daily lives. API sponsors workshops and working groups. The General Committee on Security is responsible for API's positions on industry security-related issues and works closely with government agencies responsible for the nation's security. The committee develops guidelines, seminars, and advocacy and education efforts. Committee members are the senior security managers at member companies.
	Information Management and Technology Program		Provides a comprehensive review and quantitative assessment of company security programs. Focuses on due care requirements, database of security programs, and compliance initiatives.
		Pipeline SCADA Security Standard (API Standard 1164)	Provides a model for proactive industry actions to improve the security of the Nation's energy infrastructure.
		Security Committee	Has held numerous workshops and forums to share information related to security, including the API Information Technology (IT) Security Conference for the Oil and Natural Gas Industry, Security Committee meetings (three times a year), API IT Security Forum Committee meetings (quarterly), and the Industry Hurricane Preparedness and Response Conference.
		Security in the petroleum industry	Recommends security practices for all segments of the Energy Sector.

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
Energy (Petroleum) continued		Security vulnerability assessment for the petroleum and petrochemical industries	Provides practical hands-on knowledge for performing security vulnerability assessments in multiple industries.
	API, National Petrochemical and Refiners Association (NPRA)	API/NPRA security vulnerability assessment methodology	Helps maintain and strengthen the security of personnel, facilities, and industry operations.
	Edison Electric Institute (EEI)	IT Working Group, Security Committee	Provides information and develops strategies to help electric utilities address cybersecurity threats; holds joint meetings and prepares white papers on software patch management and risk vulnerability assessments.
	EEI Security Committee		Holds workshops and forums to facilitate the exchange of security information among its members: North American Electric Reliability Corporation (NERC), government agencies, and in joint American Gas Association (AGA) Natural Gas Security Committee and EEI Security Committee meetings.
	EEI and a large group of electric utilities	Spare Transformer Sharing Agreement	More than 40 transmission facility owners developed and signed a Spare Transformer Sharing Agreement designed to require participants to maintain a specified number of high-voltage spare transformers and to provide them to other participants in the event of an act of terrorism. The spare transformers may also be used for other mutual assistance efforts. In all cases, spares that are placed in service must be replaced. On September 21, 2006, FERC issued an order that granted certain authorizations requested by the signatories to facilitate the operation of the agreement and to encourage additional participation.
	Electric Power Research Institute (EPRI)	Electricity Infrastructure Security Assessment	Provides a preliminary analysis of potential terrorist threats to the North American electricity system, together with some suggested countermeasures.
	Infrastructure Security Initiative	Infrastructure Security Initiative	Develops strategies to strengthen and protect electric power infrastructure and outline plans for rapid recovery from terrorist attacks.
	Interstate Natural Gas Association of America (INGAA)	Security Committee	Supervisory Control and Data Acquisition (SCADA) security workshops.
	The Infrastructure Security Partnership (TISP)	Guide for an action plan to develop regional disaster resilience	Developed by a TISP Task Force of more than 100 practitioners, policymakers, and technical and scientific experts from across the nation, it provides a strategy to develop the necessary level of preparedness for communities to manage major disasters. The Guide is intended for all organizations with specific missions or a vested interest in assuring that the regions in which they reside can withstand major disasters and respond and recover rapidly when the unthinkable happens.
	North American Electric Reliability Corporation (NERC)	Critical Infrastructure Protection Committee (CIPC)	Comprised of industry experts in the areas of cyber, physical, and operational security, CIPC coordinates NERC's security initiatives.

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
Energy (Petroleum) continued		Cybersecurity Standards	Provides reliability standards for information classification, identification and protection of critical cyber assets, and process control and SCADA and incident reporting. Electric Industry Cyber Security Standards are compliance based and required by FERC and the new Electric Reliability Organization (ERO).
	Electricity Sector Information Sharing and Analysis Center (ES-ISAC)		Gathers, disseminates, and interprets security-related information among industry, government, and all the sector entities.
		Industry wide critical spare equipment database	Informs companies of the location and technical characteristics of available spare transformers.
		Influenza Pandemic Planning, Preparation, and Response Reference Guide	Used by owners and operators in developing contingency plans in the event of a flu pandemic.
		Risk-Assessment Methodologies for Use in the electric utility industry	Includes background information, information on the basic components of security risk assessments, setting up a risk assessment framework, and several risk assessment methods.
		Temporary towers	Facilitates rapid restoration of transmission structures.
		Time-Stamping Guideline	Develops physical security and business network electronic connectivity.
	Northwest Power Pool (NWPP) and the Western Energy Coordination Council (WECC)	Reliability and Coordination Programs	Coordination to maintain member utilities' ability to manage risk and to implement effective security, system reliability, and recovery efforts as required ensuring public confidence.
	NPRA	Cyber Security Subcommittee	Advises and assists the Board of Directors on cybersecurity and cyber terrorism, targeting business systems and control systems in the refining and petrochemical industries.
		Security Committee	Holds workshops, tabletop exercises, and conferences to share best and effective practices related to security, including annual security conferences; workshops and forums on implementing the Maritime Transportation Security Act (MTSA); the 2006 Gulf Coast Labor Outlook; the Transportation Worker Identification Credential Program; and training courses for facility security officers on compliance with MTSA.
	National Association of Regulatory Utility Commissioners (NARUC), Regional Energy	NARUC conducts regional (multistate) energy emergency exercises involving representatives of state, local, and federal governments and industry.	Participants react to scenarios, address actions each would take, review jurisdictional issues, and examine interdependencies. Participants return to their states with tools to enhance protection and response capability.

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
Energy (Petroleum) continued	NPRA	NPRA members include more than 450 companies, including virtually all U.S. refiners and petrochemical manufacturers. NPRA speaks for the petrochemical and refining industries on issues important to their business.	NPRA seeks to inform policymakers and the public on how industries help improve their lives, strengthen the economy, protect the environment, and promote national security. It sponsors a dozen meetings, several of which are among the foremost industry meetings in the world. The NPRA Cyber Security Subcommittee advises and assists the Plant Automation and Decision Support Committee, and NPRA Board and Staff on matters pertaining to cybersecurity and cyber terrorism targeting business systems and/or control systems in the refining and petrochemical industries. It solicits and develops recommendations from NPRA members on these matters and ensures that recommendations receive consideration by concerned governmental bodies and industry groups. It develops programs on cybersecurity that are presented at NPRA cybersecurity workshops, the Plant Automation and Decision Support Conference, the NPRA Annual Meeting, and NPRA Security Conference.
	The Association of Oil Pipe Lines (AOPL)	AOPL acts as an information clearinghouse for the public, media, and pipeline industry.	AOPL provides coordination and leadership for the industry's ongoing Joint Environmental Safety Initiative. Represents common carrier crude and product petroleum pipelines in Congress, before regulatory agencies, and in the federal courts. States provide leadership in emergency response planning, training, and exercises in coordination with pipeline companies, federal regulators, and local and regional emergency response teams. State partners regularly participate in joint committees for discussing and making recommendations about risk management, compliance, damage prevention, and other issues. Provides workshops on control room security/SCADA and working groups.
	Society of Petroleum Engineers (SPE)	SPE is a professional association whose 79,000-plus members worldwide are engaged in energy resources development and production.	SPE is a key resource for technical information related to oil and gas exploration and production and provides services online and through its meetings, publications, and other programs. It provides information security wherein the technical section establishes work groups that identify and share cyber-security recommended practices in the industry. SPE's Energy Information Committee, led by former SPE President DeAnn Craig, has been working on getting members the right information and materials that they can use to dispel common misperceptions about the industry.
	Critical Infrastructure Partnership Advisory Council (CIPAC)	CIPAC membership encompasses critical CIKR owner/operator institutions and their designated trade or equivalent organizations identified as members of existing Sector Coordinating Councils (SCCs). It also includes representatives from federal, state, local, and tribal governmental entities identified as members of existing Government Coordinating Councils (GCCs) for each sector.	CIPAC facilitates effective coordination between federal infrastructure protection programs with the infrastructure protection activities of the private sector and of state, local, territorial, and tribal governments. CIPAC represents a partnership between government and CIKR owners and operators and provides a forum in which they can engage in a broad spectrum of activities to support and coordinate critical infrastructure protection.

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
Energy (Natural Gas)	Gas Technology Institute (GTI)	In an effort to protect the communications and control systems of U.S. utilities, GTI focuses on protecting the SCADA systems used throughout the natural gas industry to control unmanned operations and computer equipment.	Their research led to the GTI-recommended development of a standard industry encryption system. Results of the research were presented at the AGA Operations Conference in Chicago. The standard would incorporate GTI-selected computer algorithms to be added to both new and existing SCADA systems gas utility use to control a wide variety of operations functions. Research scientists gather about three times a year at GTI to try to figure out how to disrupt and damage America's vital natural gas systems. The experts, who have decades of experience with technology development and intimate knowledge of the inner workings of gas operations, discuss a variety of options, ranging from cyber attacks on communications systems to armed terrorist assaults. The mission: To protect. These scenario-development exercises are part of a multi-organizational effort aimed at reducing risk and enhancing the security of America's energy system. Not a new program (projects have been supported since the mid-1990s), players include AGA, DOE, gas companies, and other industry organizations (such as EPRI). For several years, GTI has taken the lead in developing technical solutions.
	Communications Sector Coordinating Council (CSCC)	Established in 2005, the broad purpose of CSCC is to foster and facilitate the coordination of sector wide activities and initiatives designed to improve physical and cybersecurity of the critical infrastructures and related information flow within the sector, cross-sector, and DHS.	Through the CSCC, private-sector owners, operators and suppliers can efficiently engage DHS and other federal agencies, collaborating to: • Identify, prioritize, and coordinate policy issues related to the protection of critical infrastructure and key resources • Facilitate sharing of information related to physical and cyber threats, vulnerabilities, incidents, potential protective measures, and recommended practices • Facilitate policy issues related to response and recovery activities and communication following an incident or event The CSCC will be a separate function from the NCC Communications ISAC (operations oriented), but will build from the experience and strengths that already exist. Separation will be established from the existing NCC responsibilities through separate meetings, management processes, and supporting infrastructure.
	AGA	Cryptographic Protection of Supervisory Control and Data Acquisition Communication.	Defines a data encryption protocol method for securing SCADA systems against possible cybersecurity attacks.
		Security Committee	Provides board-level leadership to promote security, infrastructure integrity, and reliability of the nation's natural gas utility delivery system. Oversees AGA policy in the areas of infrastructure security (physical and cyber) and operational reliability (pipeline safety and integrity management). It holds numerous workshops and forums to discuss and share security information, including the Natural Gas Security Summit, Energy IT Conference and Expo, Operations Conference, Fall Committee Meetings—Special International Security Roundtable, Leadership Conference Calls, Regional Association Conference Calls, SCADA Encryption Workshops, and joint AGA Natural Gas Security Committee and EEI Security Committee meetings.

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
Energy (Natural Gas) (continued)	AGA, INGAA, American Public Gas Association (APGA)	Security Guidelines: Natural Gas Industry, Transmission and Distribution.	Provides an approach for vulnerability assessment, critical facility definition, detection/deterrent methods, response and recovery, cybersecurity, and relevant operational standards.
Chemical	American Chemistry Council (ACC)	The Chemical Information Technology Center (ChemITC) of ACC is a forum for companies in and associated with the ACC to address common IT issues and support the industry's ability to safely and efficiently deliver products essential to society.	ACC member facilities implement, a comprehensive, multilayered security program, developed by safety and security experts, that addresses site, transportation, and cybersecurity. Under the Code, ACC members have completed vulnerability assessments, developed and implemented security plans, and verified implementation of physical enhancements through independent, third parties such as local law enforcement and emergency response officials. Security has always been a top priority for the U.S. chemical industry, and soon after the terrorist attacks of September 11, 2001, ACC member companies took the lead in securing their facilities, a critical part of our nation's infrastructure. Without waiting for government direction, ACC members adopted the Responsible Care Security Code, an aggressive plan to further enhance security of our facilities, communities and products. The Security Code, which addresses facility cyber and transportation security, requires companies to conduct comprehensive security vulnerability assessments (SVAs) of their facilities, implement security enhancements, and obtain independent verification that those enhancements have been made. The Security Code also requires companies to create security management systems, which are documented to provide quality control and assurances. Implementing the Security Code under a strict timeline is mandatory for ACC members and Responsible Care Partner companies. The Responsible Care Security Code has been widely recognized by local, state and federal governments as a model for other U.S. industries. The Cyber Security Program became one of the major strategic initiatives under ChemITC, offering manufacturers sources of information to find out what they can do to prepare to comply with new DHS regulations an to better understand how the new regulations work. It has a number of work teams dedicated to addressing important issues aligned with the Chemical Sector Cyber Security Strategy.
		Cyber Security Program Steering Team	The Cyber Security Program Steering Team manages the implementation of the Chemical Sector Cyber Security Strategy, chartering project teams, and carrying out Program plans and activities. Each steering team member is aligned with a cybersecurity work team. A major part of their role includes providing leadership for projects in support of the Chemical Sector Cyber Security Strategy and driving the Program's overall goal of sector wide adoption of cybersecurity practices and guidance (http://www.americanchemistry.com/s_responsiblecare/doc.asp?CID=1298&DID=5085).
		Communication Material and Outreach Team	This project team creates rich, value-added opportunities for chemical industry cybersecurity professionals to gather and share experiences about cybersecurity challenges. It supports other project teams as they develop documents and communications to increase understanding of cybersecurity issues, as well as facilitate the use of available cybersecurity tools and guidance. This team also facilitates widespread adoption of cybersecurity guidance within chemical sector trade associations, their member companies, and supply chain partners, and builds and maintains the credibility of the chemical sector's cybersecurity effort.

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
Chemical (continued)		European Networking and Implementation Team	Recognizing the global nature of the chemical industry, this team brings together European IT and manufacturing control systems security professionals to understand and address regional cybersecurity needs. The team focuses on providing networking opportunities on cybersecurity topics of specific interest to the European community and increasing the number of European-based companies that participate in cybersecurity activities. The team has initiated a data privacy project designed to improve networking discussions regarding government data privacy initiatives and create a guidance document focused on general data privacy methodologies. The team also determines how best to work with recognized organizations in Europe including VCI and CEFIC to understand and address evolving cybersecurity requirements and needs
		Information Technology Team	This project team was revitalized in late 2007 as a forum for ChemITC® Charter and Affiliate members to share ideas and experiences regarding the secure use of information technology. This team works to establish chemical sector and cross sector dialogue on various IT security topics, maintaining a focus on technology itself, rather than people or process issues. The team looks to ChemITC Affiliate members for their perspectives on IT security issues facing chemical companies today, and in turn promotes active affiliate member interaction with other members. During the course of the year, the team works toward a number of deliverables, which may include coordinating Webinars and panel discussions, creating guidance documents or white papers, and other activities on key topics of interest.
		Manufacturing and Control Systems Security Team.	This project team acts as the "voice of the Program" in matters related to the definition, development, and application of cybersecurity technologies and methods to manufacturing and control systems. It collects, identifies, and facilitates the use of practices for securing manufacturing and control systems and establishes a network of manufacturing and control systems subject matter experts. This team contributes manufacturing and control system expertise to various program projects by identifying and advocating features and technologies that improve manufacturing and control system security. It also represents chemical sector interests in outside organization's development of industry practices and standards for manufacturing and control systems security, including the ISA SP-99 committee, the NIST Process Control Systems Requirements Forum, the DHS-sponsored Process Control Systems Forum, Idaho National Laboratory's Control Systems Security Center, and others.
		Risk Assessment and Preparedness Team	This team is fully resourced at this time, but should consider participating in another Cyber Security Program Work Team.

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
Chemical (continued)	Instrumentation, Systems, and Automation Society (ISA)	Founded in 1945, and based in Research Triangle Park, North Carolina, ISA is a leading, global, nonprofit organization that is setting the standard for automation by helping over 30,000 worldwide members and other professionals solve difficult technical problems, while enhancing their leadership and personal career capabilities.	ISA develops standards; certifies industry professionals; provides education and training; publishes books and technical articles; and hosts the largest conference and exhibition for automation professionals in the Western Hemisphere. ISA is the founding sponsor of The Automation Federation (http://www.automationfederation.org). The working group (WG1) identifies security vulnerabilities addressed by this technology, typical deployment, known issues and weaknesses, assessment of use in manufacturing and control system environment, future directions, recommendations and guidance, and references.
		ISA-99 Committee	The ISA-99 Committee addresses manufacturing and control systems whose compromise could result in any or all of the following situations: • endangerment of public or employee safety • loss of public confidence • violation of regulatory requirements • loss of proprietary or confidential information • economic loss • impact on national security A member of ChemITC served on this committee.
		ISA Security Compliance Institute	The ISA Security Compliance Institute ensures that industrial control system products and services comply with industry standards and practices, "Development of tests specifications and methodologies based on available standards and practices"
	American Gas Association (AGA), Gas Technology Institute (GTI), and NIST 12 Guidance	Cryptographic guidelines for SCADA communication	• AGA 12, Parts 1 and 2 working guidelines released (2003–2005) • AGA 12, Parts 3 and 4 under development
	America Petroleum Institute (API)	API is a member of the SCC and a trade association for the oil and natural gas industry.	As an industry forum, research center, and policy input institute, API developed API standard 1164, Pipeline SCADA Security (2004).
	ACC, Chlorine Institute, and Synthetic Organic Chemical Manufacturers Association	Site Security Guidelines (SSG)	Developed the Site Security Guidelines (SSG) to address many transportation functions that occur at or within the boundaries of fixed chemical sites (http://www.chlorineinstitute.org/files/PDFs/trnsecurguidnce06-02.pdf?snItemNumber=2463).

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
Chemical (continued)	The Chemical Sector Coordinating Council (SCC)	The CSCC is made up of 17 member trade associations and an owner/operator chair and vice-char. The CSCC serves as central point of private sector security information sharing and also act as the liaison to the federal government.	The CSCC represents a primary point of entry for government into the sector for addressing the entire range of CIKR protection activities and serves as a strategic communications and coordination mechanism between CIKR owners, operators, and suppliers, and, as appropriate, with the government during emerging threats or response and recovery operations, as determined by the sector. The CSCC supports the information-sharing capabilities and mechanisms for the sector. Additionally the council participates in planning efforts related to the development, implementation, update, and revision of the SSPs and review of the Sector Annual Reports.
	National Petrochemical and Refiners Association (NPRA)	NPRA members include more than 500 companies, including virtually all U.S. refiners and petrochemical manufacturers. Its members supply consumers with a wide variety of products used daily in their homes and businesses. NPRA is a member of the CSCC	NPRA has a Plant Automation & Decision Committee which advises the Board of Directors and the NPRA staff on information technology issues. The committee develops the program for the annual NPRA Plant Automation and Decision Support Conference which focuses on practical experience with the application and management of information technology in areas including process control, modeling, IT networks, and Internet-based applications. The committee also has a Cyber Security Subcommittee to provide information and recommendations to the Plant Automation and Decision Support Committee on matters pertaining to cyber security and cyber terrorism targeting business systems and/or control systems in the refining and petrochemical industries. The subcommittee also develops the program for the Cyber Security Workshop.
	Chlorine Institute (CI)	The Chlorine Security Leadership Team (Team), created in 2004, is a partnership between CI and the Chlorine Chemistry Council (Council). The Council is a valuable tool to enable the government to accurately understand the status and views of the chemical sector.	The Team advances the coordination of security policy and related communication with stakeholders, research initiatives, and member services in order to enhance the security of chlorine and understand that it is a critical asset to public health and the national security. The Council advances the protection of chemistry and chemical manufacturing as a critical infrastructure by facilitating the two-way sharing of information about physical and cyber threats, vulnerabilities, incidents, protective measures and recommended practices.
	Chemical Producers & Distributors Association (CPDA)	CPDA is a voluntary, nonprofit membership organization in the U.S. consisting of 73 member companies engaged in the manufacture, formulation, distribution and sale of some $5 billion worth of crop protection chemicals, fertilizers, adjuvant and inert ingredients used in food, feed, and fiber crops, the care and maintenance of lawns, gardens and turf, and in various forestry and vegetation management markets.	CPDA held a security preparedness workshop to address the pesticide industry's specific concerns after September 11th. CPDA brought in a range of experts who outlined (1) procedures a company should take to minimize its risk of being targeted, (2) the how's and why's of being prepared to cope with a potential attack, and (3) continuing on both a business and personal level after an attack occurs. While sharing a concern for cyber attacks, the theme of "coordinated communication" also emerged from the workshop. Three types of communication are necessary: (1) within a company before an event (preparedness), (2) between a company and its community, including its customers and neighbors, law enforcement, and the health care community, and (3) between a company and government agencies.

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
Chemical (continued)	Agricultural Retailers Association (ARA)	ARA advocates before Congress and the Executive Branch to ensure a profitable business environment for members.	ARA, CropLife America (CLA) and The Fertilizer Institute [TFI]) in cooperation with Asmark Institute, has produced a new Web-based tool which will assist agribusiness retailers in conducting a security vulnerability assessment on their retail facility and their transportation practices. This SVA is a tool to use to identify and assess potential security threats, risks and vulnerabilities. The SVA tool designed by Asmark Institute, a member of the Agricultural Retailers Association, has granted to ARA the license and use of the Web-based program. ARA in turn has offered to share the SVA with the Agribusiness Security Working Group.
	Chemgard	ChemGard was formed by a vote of the Iowa InfraGard membership at the November 2007 Quarterly meeting to provide a basis for threat information dissemination, share security recommended practices and initiatives, and collaborate to protect against and recover from natural and man-made disasters.	ChemGard focuses on assisting InfraGard members responsible for security and continuity of operations at Chemical and Industrial facilities, working to communicate and coordinate efforts to maximize protection of Iowa's industrial base. Its goal is to add to Iowa's InfraGard Chapter to broaden collective experience, knowledge, and resources. In 2008 it plans to begin meeting throughout the state and identify opportunities to enhance security and infrastructure protection through sharing of security recommended practices, threat and vulnerability information, and educational resources. ChemGard is working with Iowa's Homeland security Chemical Sector Workgroup to develop an Iowa Chemical Sector Specific Plan to partner with the Federal Chemical Sector Specific Plan.
	CIPAC	Chemical Joint Sector Committee membership encompasses CIKR owner/operator institutions and their designated trade or equivalent organizations that are identified as members of existing Sector Coordinating Councils (SCCs).	The Chemical Joint Sector Committee, which includes representatives from federal, state, local and tribal governmental entities identified as members of existing Government Coordinating Councils (GCCs) for each sector, facilitates effective coordination between federal infrastructure protection programs with the infrastructure protection activities of the private sector and of state, local, territorial, and tribal governments.
Nuclear	Nuclear Consultation Working Group	The Working Group is comprised of leading experts in environmental risk, radiation waste, energy policy, energy economics, political science, social science, environmental justice, and democratic involvement.	The Working Group speaks with one collective voice to achieve nuclear initiatives.
	Nuclear Defense Working Group (NDWG)	NDWG is a vehicle to clarify needs among the Domestic Nuclear Detection Office, Congress, and other agencies. NDWG is funded by a grant from a private foundation, thus assuring its independence and honest-broker status.	Several meetings with experts in relevant technology, policy, and operational areas are planned during 2008 to review U.S. efforts to prevent and/or defend against clandestine nuclear attack and to improve congruence between Executive Branch efforts and Congressional oversight responsibilities. Project leadership will produce a series of papers based on conclusions reached in these discussions, which will focus on topics such as long-term commitments to transformational R&D, the reinvigoration of national nuclear laboratories, and institutionalizing net assessments for combating smuggled nuclear weapons. Members of the NWDG and the Center's project leadership will share its findings, as appropriate, with Congressional leaders, senior staff, and top decision makers in the Executive Branch.

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
Nuclear (continued)	Electric Power Research Institute (EPRI)	EPRI's members represent more than 90% of the electricity generated in the U.S. International participation in its programs includes 40 countries. As a nonprofit organization.	EPRI brings scientists, engineers, and experts from academia, industry, and other research centers together to meet challenges in electricity generation, delivery, and use. EPRI conducts R&D on technology, operations, and the environment for the global electric power sector. It supports multidiscipline research in emerging technologies, which drives long-range research and development planning.
	The Institute for Information Infrastructure Protection (I3P)	I3P is a consortium of leading universities, national laboratories, and nonprofit institutions dedicated to strengthening the U.S. cyber infrastructure.	Since 2005, the I3P has increased efforts and resources to actively coordinate and fund cybersecurity research to help secure U.S. critical information infrastructures. Two multi-institutional research projects have been funded that target process control systems and the economics of cybersecurity. Research topics were selected through open dialogue within the consortium, which considered gaps in national efforts, the criticality of the topic, and the impact I3P could have. Research is conducted by teams composed of multiple consortium members, which is a hallmark of all I3P research projects. Each project has a team leader who has overall responsibility for the project, particularly for meeting milestones and producing deliverables. Team leaders are in regular communication with the I3P Chair and administrative office on progress, funding questions, and other challenges as they arise.
	Multi-State Information Sharing and Analysis Center (MS-ISAC)	MS-ISAC is a voluntary and collaborative organization with participants from all 50 states and the District of Columbia. Its mission, which is consistent with the objectives of the *National Strategy to Secure Cyberspace*.	MS-ISAC provides a common mechanism for raising the level of cybersecurity readiness and response in each state and within local governments, serves is a central resource for gathering information on cyber threats to critical infrastructure from states, and provides for two-way sharing of information between and among the states and with local governments. It disseminates early warnings of cyber system threats ,shares security incident information, provides trending and other analysis for security planning, distributes current proven security practices and suggestions, promotes awareness of the interdependencies between cyber and physical critical infrastructure between and among the different sectors. The MS-ISAC serves as the liaison between the states and DHS's US-CERT for cyber incident reporting.
	American Society for Cybernetics (ASC)	The ASC emphasizes the role of regular gatherings to foster understanding by exchanging ideas.	ASC sponsors conferences and other occasional events to provide the multidisciplinary field of cybernetics a focal venue for such interactions.
	International Facility Management Association (IFMA)	Formed in 1980, IFMA is the world's largest and most widely recognized international association for professional facility managers. It supports over 19,000 members in 60 countries represented in 125 chapters and 15 councils worldwide.	IFMA manages more than 37 billion square feet of property and annually purchases more than $100 billion in products and services. IFMA certifies facility managers, conducts research, provides educational programs, recognizes facility management degree and certificate programs and produces World Workplace—the world's largest facility management conference and exposition.

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
Nuclear (continued)	Instrumentation, Systems, and Automation Society (ISA)	As a leading, global, nonprofit organization, ISA is the founding sponsor of The Automation Federation, which develops and provides criteria for procuring and implementing secure control systems.	ISA is setting the standard for automation by helping over 30,000 worldwide members and other professionals solve difficult technical problems, while enhancing their leadership and personal career capabilities. ISA develops standards, certifies industry professionals, provides education and training, publishes books and technical articles, and hosts the largest conference and exhibition for automation professionals in the Western Hemisphere.
Water	American Waterworks Association (AWWA),	AWWA, headquartered in Denver, Colorado, provides about 85% of the North American population with safe drinking water. It has more than 57,000 members in 43 sections, including 100 countries outside North America.	AWWA members host dozens of events every year covering all aspects of water and wastewater, from management and research to conservation, operations, and engineering.
	Association of Metropolitan Water Agencies (AMWA),	AMWA is an organization of the largest publicly-owned drinking water systems in the U.S. It was organized to ensure that the issues of large publicly owned water suppliers would be represented in Washington, D.C.	AMWA's membership serves more than 127 million Americans with drinking water from Alaska to Puerto Rico. AMWA is the nation's only policy-making organization solely for metropolitan drinking water suppliers. AMWA is the industry lead for the Water Sector and oversees the Water Information Sharing and Analysis Center (WaterISAC) and Water Security Channel (WaterSC).
	National Association of Clean Water Agencies (NACWA)	NACWA represents the interests of over 300 public agencies and organizations that collectively pursue scientifically based technically sound and cost effective laws and regulations.	NACWA members serve the majority of the population in the United States and collectively treat and reclaim more than 18 billion gallons of wastewater daily. NACWA maintains a key role in the development of environmental legislation, and works closely with federal regulatory agencies in the implementation of environmental program.
	National Association of Water Companies (NAWC)	Founded in 1895, NAWC represents all aspects of the private water service industry. Its member businesses include ownership of regulated drinking water and wastewater utilities and the many forms of public-private partnerships and management contract arrangements.	NAWC maintains an aggressive set of programs to support the Private Water Service Industry and their customers. It provides the means to assure that its members concerns and the concerns of their customers are before the nation's key decision makers. The association's relations with federal legislators and agency directors, as well as with Public Utility Commissions and staff, improve members' effectiveness in addressing the common concerns of the industry, its customers, and the nation.

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
Water (continued)	National Water Resources Association (NRWA)	NRWA is a nonprofit federation of state associations, individuals, and agencies who advocate federal policies, legislation, and regulations promoting protection, management, development and beneficial use of water resources for its members.	NWRA works to balance the needs of people and the environment by working closely with Congress and the Executive Branch to establish positive relationships with key resource management agencies and departments. Its top priorities for the 110th Congress include the fair and reasonable implementation of the Endangered Species Act and Clean Water Act and the maximum full funding of water project and program needs on an agency-wide basis.
	Water Environment Federation (WEF)	WEF is a not-for-profit technical and educational organization with more than 34,000 individual members and 81 affiliated Member Associations representing an additional 50,000 water quality professionals throughout the world.	WEF and its member associations work to preserve and enhance the global water environment. WEF tracks, monitors and actively comments on legislation impacting clean water issues. WEF works closely with its membership to educate Congress on clean water issues impacting their districts and States. As a leading source of water quality expertise, WEF advances the water quality profession by providing access to the world's best science, engineering, and technical practices in the water environment field.
	Water Environment Research Foundation (WERF)	WERF manages independent scientific research that leads to cost effective responses to water quality concerns affecting the environment and human health.	For nearly 20 years WERF has contributed to the global scientific and technological body of knowledge addressing water quality issues encompassed by wastewater treatment and conveyance, infrastructure and asset management, water reclamation and reuse, biosolids, stormwater, and watersheds.
	American Water Works Association Research Foundation (AwwaRF)	AwwaRF is a member-supported, international, nonprofit organization that sponsors research to enable water utilities, public health agencies, and other professionals to provide safe and affordable drinking water to consumers.	AwwaRF works to advance the science of water to improve the quality of life by (1) sponsoring an anticipatory and scientifically credible research program that is responsive to the needs of the water supply community; (2) identifying the practical benefits of research findings and delivering this knowledge to stakeholders throughout the water supply community; and (3) cultivating partnerships with organizations around the world to leverage funding and share expertise.
	American Public Works Association (APWA)	APWA is an international educational and professional association of public agencies, private sector companies, and individuals dedicated to providing high quality public works goods and services.	APWA provides a forum in which public works professionals can exchange ideas, improve professional competency, increase the performance of their agencies and companies, and bring important public works-related topics to public attention in local, state and federal arenas.
	Association of Public Health Laboratories (APHL)	APHLs work to strengthen laboratories serving the public's health in the U.S. and globally.	Public health laboratories serve as laboratory first responders, protecting the public from diseases and environmental health hazards. Avian influenza, anthrax, contaminated water and *E. coli* have all been the subject of their investigations. In an effort to strengthen the Nation's laboratory capability and capacity, EPA and APHL have formed a partnership to formulate sound public health and environmental policies, offer training and education, and improve overall laboratory management and practices nationwide.

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
Water (continued)	Association of State and Territorial Health Officials (ASTHO)	ASTHO is a national nonprofit organization dedicated to formulating and influencing sound public health policy, and to assuring excellence in state-based public health practice.	ASTHO formulates and influences sound national public health policy and helps state health departments develop and implement programs and policies to promote health and prevent disease. It addresses a variety of key public health issues and publishes newsletters, survey results, resource lists, and policy papers that assist states in the development of public policy and in the promotion of public health programs at the state level.
	Environmental Council of the States (ECOS)	ECOS is the national nonprofit, nonpartisan association of state and territorial environmental agency leaders. Its mission is to improve the capability of state environmental agencies and their leaders to protect and improve human health and the environment of the United States of America.	ECOS works to accomplish its mission by (1) articulating, advocating, preserving, and championing the role of the states in environmental management; (2) Providing for the exchange of ideas, views and experiences among states and others; (3) fostering cooperation and coordination in environmental management; and (4) articulating state positions to Congress, federal agencies, and the public on environmental issues.
	International City/County Management Association (ICMA)	ICMA is a premier local government leadership and management organization whose mission is to create excellence in local governance by advocating and developing the professional management of local government worldwide.	In addition to supporting its nearly 9,000 members, ICMA provides publications, data, information, technical assistance, and training and professional development to thousands of city, town, and county experts and other individuals throughout the world.
	National Association of Counties (NACo)	NACo was formed to stimulate the continuing improvement of county government; speak nationally for county government, contribute to the knowledge and awareness of the heritage and future of county government, serve as a liaison between the nation's counties and other levels of government, and achieve public understanding of the role of counties in a federal system.	NACo seeks to achieve it mission by sponsoring conferences, exchanging information and advice, and conducting other activities that benefit county government and improve service to the public rendered by county government. NACo provides an extensive line of services including legislative, research, technical, and public affairs assistance, as well as enterprise services to its members. It acts as a liaison with other levels of government, works to improve public understanding of counties, serves as a national advocate for counties and provides them with resources to help them find innovative methods to meet the challenges they face. NACo is involved in a number of special projects that deal with such issues as homeland security, drug abuse and broader access to health care.
	National Association of County and City Health Officials (NACCHO)	NACCHO is the national organization representing local health departments.	NACCHO supports efforts that protect and improve the health of all people and all communities by promoting national policy, developing resources and programs, seeking health equity, and supporting effective local public health practice and systems. NACCHO represents local public health agencies, including city, county, metropolitan, district, and tribal agencies.

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
Water (continued)	National Conference of State Legislatures (NCSL)	NCSL is a bipartisan organization that serves the legislators and staffs of the nation's 50 states, its commonwealths and territories.	NCSL provides research, technical assistance and opportunities for policymakers to exchange ideas on the most pressing state issues. NCSL is an effective and respected advocate for the interests of state governments before Congress and federal agencies.
Wastewater	National Association of Clean Water Agencies (NACWA)	NACWA represents the interests of over 300 public agencies and organizations that collectively pursue scientifically based technically sound and cost effective laws and regulations.	NACWA members serve the majority of the population in the United States and collectively treat and reclaim more than 18 billion gallons of wastewater daily. NACWA maintains a key role in the development of environmental legislation, and works closely with federal regulatory agencies in the implementation of environmental program.
	Wastewater Treatment Plant Operator On-Site Assistance Training Program	This program was implemented to address the problem of non-compliance at small publicly-owned wastewater treatment plants, with a discharge of less than 5 million gallons per day, through direct on-site training and other operation and maintenance assistance.	Program trainers provide financial, technical, and operations and maintenance (O&M) assistance to small municipal wastewater treatment plants through direct onsite operator training. The program identifies any need to repair or build new facilities to meet existing or future permit limits, assists the town during the process of selecting consultants and design review, recommends ways to improve preventive maintenance of equipment and structures, and often reduces energy and chemical costs through more efficient operation techniques.
	Water Environment Federation (WEF)	WEF is a not-for-profit technical and educational organization with more than 34,000 individual members and 81 affiliated Member Associations representing an additional 50,000 water quality professionals throughout the world.	WEF and its member associations work to preserve and enhance the global water environment. WEF tracks, monitors and actively comments on legislation impacting clean water issues. WEF works closely with its membership to educate Congress on clean water issues impacting their districts and States. As a leading source of water quality expertise, WEF advances the water quality profession by providing access to the world's best science, engineering, and technical practices in the water environment field.
	Water Environment Research Foundation (WERF)	WERF manages independent scientific research that leads to cost effective responses to water quality concerns affecting the environment and human health.	For nearly 20 years WERF has contributed to the global scientific and technological body of knowledge addressing water quality issues encompassed by wastewater treatment and conveyance, infrastructure and asset management, water reclamation and reuse, biosolids, stormwater, and watersheds.
Dams	Association of State Dam Safety Officials (ASDSO)	A national non-profit organization serving state dam safety programs and the broader dam safety community	ASDSO advances and improves the safety of dams by supporting the dam safety community and state dam safety programs, raises awareness of dam safety issues, facilitates cooperation, provides a forum for the exchange of information, represents dam safety interests before governments, provides outreach programs, and creates a unified community of dam safety advocates.

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
Dams (continued)	National Association of Flood and Stormwater Management Agencies (NAFSMA)	NAFSMA is an organization of public agencies whose function is the protection of lives, property, and economic activity from the adverse impacts of storm and flood waters.	The mission of the Association is to advocate public policy, encourage technologies, and conduct education programs which facilitate and enhance the achievement of the public service function of its members.
	Association of State Floodplain Managers (ASFPM)	ASFPM is an organization of professionals involved in floodplain management, flood hazard mitigation, National Flood Insurance Program, and flood preparedness, warning and recovery	ASFPM represents the flood hazard specialists of local, State, and Federal government, research community, insurance industry, and the fields of engineering, hydrologic forecasting, emergency response, water resources, and others.
	CEATI International, Inc.	CEATI provides leadership in developing applied technology solutions for the electricity industry. CEATI International facilitates funding leveragability through the creation of project consortiums.	CEATI International Inc. brings electrical utility industry professionals together, through focused interest groups and collaborative projects, to identify and address technical issues that are critical to their organizations. Participants can undertake projects that respond to their strategic goals at a fraction of the cost of doing so independently. The need for international breadth and inter-industry applicability in technology development is addressed through a practical, dynamic, and cost effective program. It operates 15 interest groups covering power generation, transmission, distribution, and use.
	Network for Earthquake Engineering Simulation Cyberinfrastructure (NEESit)	The NEES Cyberinfrastructure Center (NEESit) is a service-focused organization created to deliver information technology tools and infrastructure to enable earthquake engineers to remotely participate in experiments, perform hybrid simulations, organize and share data, and collaborate with colleagues.	NEESit manages an education, outreach, and training program. Manages the shared-use maintenance and operations budget for equipment sites. Facilitates the scheduling of NEESit research activities at equipment sites. Manages the system wide information technology infrastructure of the NEES Collaboratory, providing access to a broad range of users. Maintains repositories for NEESit data and simulation tools program and advances NEESit infrastructure capabilities through the pursuit of opportunities for technology development. Fosters linkages and partnerships with federal, state, and local government entities, national laboratories, the private sector, and international collaborators. It also facilitates advanced research usage of NEESit.
	International Commission on Large Dams (ICOLD)	ICOLD is a nongovernmental International Organization that provides a forum for the exchange of knowledge and experience in dam engineering.	The Organization leads the profession in ensuring that dams are built safely, efficiently, economically, and without detrimental effects on the environment. ICOLD encourages advances in the planning, design, construction, operation, and maintenance of large dams and their associated civil works, by collecting and disseminating relevant information and by studying related technical questions.
	United States Society on Dams (USSD)	USSD works to be the nation's leading organization of professionals dedicated to advancing the role of dams for the benefit of society.	Among other things, USSD examines contemporary dam issues, such as dam safety, environmental impacts and dam decommissioning, publishes technical reports and contributes to ICOLD publications, distributes ICOLD Publications within the United States, participates in and contributes to international seminars on dams, holds an Annual Meeting and Conference, exhibition and study tour, and collects statistics and information about U.S. dams (highest dams, largest hydro projects and largest reservoirs).

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
Dams (continued)	International Energy: Hydro Electricity (IEAHydro)	IEAHydro is a working group of IEA member countries that have a common interest in advancing hydropower worldwide.	IEAHydro encourages knowledge through awareness and supports the sustainable use of water resources for the development and management of hydropower. Activities include developing technical reports, new hydro projects, and education and training materials that demonstrate the potentials and strengths of a learning management system in web-based training and exchange of information. A Public Awareness task force set up the first IEAhydro website to promote the work of the Implementing Agreement, and to offer resources for both hydro professionals and non-professionals. Another team developed an extensive database of hydropower success stories in design, operation, and mitigation.
Transportation	Transportation Community Awareness and Emergency Response (TRANSCAER)	TRANSCAER is a voluntary national outreach effort that focuses on assisting communities to prepare for and respond to a possible HAZMAT transportation incident. TRANSCAER members are volunteer representatives from the chemical manufacturing, transportation, distribution, and emergency response industries, as well as the government.	Each year, at hundreds of sites nationwide, TRANSCAER provides thousands of emergency responders and local officials with unique, hands-on training using actual transportation equipment. Training includes hands-on and classroom activities; topics Include chlorine, hydrochloric acid, sodium hypochlorite, sodium hydroxide, railroad safety/emergency response and more.
	Railway Alert Network (RAN)	RAN is a DOD-certified, 24/7 Operations Center, working at the Secret level to monitor and evaluate intelligence on potential threats and communicate with railroads through the Railway Alert Network (RAN).	RAN is controlled by the Association of American Railroads (AAR) Operations Center, which links federal national security and military personnel, and major customer associations with the freight railroad.
	AAR Operations Center	The AAR Operations Center operates RAN through which AAR declares appropriate AAR freight railroad security alert levels.	The AAR Operations Center collects, analyzes, and disseminates information on physical threats to railroad operations on a 24 hours per day, 7 days per week (24/7) basis.
	American Petroleum Institute (API)	API is the only national trade association representing the entire the oil and natural gas industry.	Our industry's major segments encompass all the steps involved in finding, producing, processing, transporting, and marketing oil and natural gas.
	Association of Oil Pipelines (AOPL)	As a trade association, AOPL: Acts as an information clearinghouse for the public, the media and the pipeline industry.	AOPL provides coordination and leadership for the industry's ongoing Joint Environmental Safety Initiative, Represents common carrier crude and product petroleum pipelines in Congress, before regulatory agencies, and in the federal courts.

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
Transportation (continued)	American Gas Association (AGA)	AGA enhances communications between AGA staff and members and serves as a key electronic tool for dissemination of information and services. AGA represents companies delivering natural gas to customers to help meet their energy needs.	AGA (1) advocates natural gas issues that are priorities for its members and that are achievable (2) encourages, facilitates and assists members in sharing information designed to achieve operational excellence by improving their safety, security, reliability, efficiency, and environmental and other performance metrics; (3) assists members in managing and responding to customer energy needs, regulatory trends, natural gas markets, capital markets and emerging technologies; (4) collects, analyzes, and disseminates data on a timely basis to policy makers; (5) serves as a voice on behalf of the energy utility industry and promotes natural gas demand growth; and (6) delivers measurable value to AGA members.
	American Public Gas Association (APGA)	APGA is an advocate for publicly-owned natural gas distribution systems, and educates and communicates with members to promote safety, awareness, performance, and competitiveness.	APGA represents the interests of public gas before Congress, federal agencies, and other energy-related stakeholders by developing regulatory and legislative policies that further the goals of its members. It also organizes meetings, seminars, and workshops with a specific goal to improve the reliability, operational efficiency, and regulatory environment in which public gas systems operate.
	Interstate Natural Gas Association of America (INGAA)	INGAA is a trade organization that advocates regulatory and legislative positions of importance to the natural gas pipeline industry in North America.	INGAA facilitates the efficient, cost-effective and environmentally responsible construction of new natural gas pipelines and the safe and reliable operation of the North American natural gas pipeline system in order to advance the delivery of natural gas for the benefit of the consuming public, the economy, and the environment.
	Natural Resources Canada (NRCan)	NRCan works to ensure the responsible development of Canada's natural resources, including energy, forests, minerals and metals. We also use our expertise in earth sciences to build and maintain an up-to-date knowledge base of our landmass and resources.	NRCan develops policies and programs that enhance the contribution of the natural resources sector to the economy and improve the quality of life for all Canadians. It conducts innovative science in facilities across Canada to generate ideas and transfer technologies. It also represents Canada at the international level to meet the country's global commitments related to natural resources. NRCan provides access to a rich and diverse array of information on the responsible development of Canada's natural resources, including maps, image and data collections, publications, and library and reference collections. Natural Resources Canada collects and shares information on fuel efficiency and environmentally responsible vehicles and practices for commercial use and for Canadians.
	Gas Technology Institute (GTI)	GTI is the leading research, development and training organization serving the natural gas industry and energy markets.	GTI provides products, services and information that help customers solve problems or capitalize on opportunities related to finding, producing, delivering, and using natural gas and other energy resources.
ISACs	Information Technology Information Sharing and Analysis Center (IT-ISAC)	IT-ISAC is a trusted community of security specialists from companies across the Information Technology industry dedicated to protecting the IT infrastructure.	Activities include reporting and exchanging information concerning electronic incidents, threats, attacks, vulnerabilities, solutions and countermeasures, recommended security practices and other protective measures; establish a mechanism for systematic and protected exchange and coordination of such information; and provide thought leadership to policymakers on cybersecurity and information sharing issues.

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
ISACs (continued)	Information Technology Sector Coordinating Council (IT-SCC)	IT-SCC brings companies, associations, and other key IT sector participants together to coordinate strategic activities and communicate broad sector member views associated with infrastructure protection, response, and recovery that are relevant to the IT Sector.	IT-SCC (1) coordinates the integration of broad sector perspectives on CIP policy and Strategy; (2) facilitates improved global security for the network of networks underpinning the IT infrastructure and for other sectors and governments that depend upon it; (3) improves understanding (among governments and other entities) of IT sector issues associated with CIP; (4) enhances public confidence in the reliability and integrity of information technologies, infrastructures and services and security of personal information; and (5) improves IT sector coordination with other sector groups and government agencies—International efforts include working with international members and other governments on CIP issues if appropriate.
	National Cyber Security Partnership (NSCP)	NCSP is a public-private partnership that develops shared strategies and programs to better secure and enhance America's critical information infrastructure.	NCSP established five task forces comprised of cybersecurity experts from industry, academia and government. Each task force is led by two or more co-chairs. The NCSP-sponsoring trade associations act as secretariats in managing task force work flow and logistics. The task forces include: Awareness for Home Users and Small Businesses, Cyber Security Early Warning, Corporate Governance, Security Across the Software Development Life Cycle, and Technical Standards and Common Criteria.
Information Technology and Communications Sectors	The Information Technology Information Sharing and Analysis Center (IT-ISAC)	IT-ISAC is a trusted community of security specialists from companies across the Information Technology industry dedicated to protecting the Information Technology infrastructure.	Daily conference calls with members sharing incident and response information. Activities include reporting and exchanging information concerning electronic incidents, threats, attacks, vulnerabilities, solutions and countermeasures, recommended security practices and other protective measures; establish a mechanism for systematic and protected exchange and coordination of such information; and provide thought leadership to policymakers on cybersecurity and information sharing issues. The IT-ISAC maintains a 24/7 operations center for collecting and disseminating incident and alert information with its members. Control systems security relevance is provided through participation of the DHS Control Systems Security Program in the daily situational awareness calls and through US-CERT.
	Information Technology Sector Coordinating Council (ITSCC)	IT-SCC brings companies, associations, and other key IT sector participants together to coordinate strategic activities and communicate broad sector member views associated with infrastructure protection, response, and recovery that are relevant to the IT Sector.	IT-SCC (1) coordinates the integration of broad sector perspectives on CIP policy and Strategy; (2) facilitates improved global security for the network of networks underpinning the information technology infrastructure and for other sectors and governments that depend upon it; (3) improves understanding (among governments and other entities) of IT sector issues associated with CIP; (4) enhances public confidence in the reliability and integrity of information technologies, infrastructures and services and security of personal information; and (5) improves IT sector coordination with other sector groups and government agencies—International efforts include working with international members and other governments on CIP issues if appropriate.
	National Cyber Security Partnership (NCSP)	NCSP is a public-private partnership that develops shared strategies and programs to better secure and enhance America's critical information infrastructure.	NCSP established five task forces comprised of cybersecurity experts from industry, academia and government. Each task force is led by two or more co-chairs. The NCSP-sponsoring trade associations act as secretariats in managing task force work flow and logistics. The task forces include: Awareness for Home Users and Small Businesses, Cyber Security Early Warning, Corporate Governance, Security Across the Software Development Life Cycle, and Technical Standards and Common Criteria. These programs are primarily focused on IT cybersecurity with relevance to common issues in control systems vulnerabilities and mitigations.

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
Information Technology and Communications Sectors (continued)	Internet Security Alliance	The Internet Security Alliance (ISAlliance) was created to provide a forum for information sharing and thought leadership on information security issues.	The Internet Security Alliance is a non-profit collaboration between the Electronic Industries Alliance (EIA), a federation of trade associations, and Carnegie Mellon University's CyLab. The alliance develops and provides security focused products and training to its members. Examples include the Enterprise Integration Program that integrates security throughout corporate structures by examining complex compliance issues, like Outsourcing Risk Management, Breach Notification, Incident Handling, through a multidisciplinary perspective considering Technical, Legal/Regulatory, Business Operational, and Policy issues. No specific control systems security programs or activities were identified; however, cybersecurity issues and programs exist through the vendors and trade organizations and at Carnegie Mellon University.
	Communications Sector Coordinating Council (CSCC)	The CSCC has the analogous role of the IT-SCC for telecommunications systems comprised of principal providers of communications services and equipment.	The CSCC is separate from the NCC Communication ISAC to work as the coordinating component of the Partnership for Critical Infrastructure Security under the CIPAC. Programs include working groups for Administration, State and Local, Cyber, Measurement, Outreach and planning and reporting. Members from the IT-SCC and the CSCC participate in cross sector coordination. No specific control systems security programs or activities were identified; however, cybersecurity issues and programs exist through the vendors and communications trade organizations.
	National Coordinating Center for Telecommunications	NCC is the designated an ISAC for Telecommunications. The NCC-ISAC will facilitate the exchange among government and industry participants regarding vulnerability, threat, intrusion, and anomaly information affecting the telecommunications infrastructure.	The NCC coordinates the restoration and provisioning of NS/EP telecommunication services and facilities during natural disasters and armed conflicts. Industry participants include all the major communications providers and manufacturers of equipment. Programs include the Government Emergency Telephone Service (GETS), Telecommunications Priority Service (TSP), Shared Resources High Frequency Radio Program (SHARES), and the National Telecommunications Coordinating Network (NTCN). No specific control systems security programs or activities were identified; however, cybersecurity issues and programs exist through the vendors and communications trade organizations.
Postal and Shipping	Postal and Shipping Sector Coordinating Council	Comprised of the principal shippers of mail and packages: DHL, United States Postal Service, United Parcel Service, and Federal Express.	No specific control systems activities have been identified however; the sector participants are heavily involved in the use of automation and networked systems for tracking and delivery processing. Companies such as the United Parcel Service and Federal Express develop and provide logistic tools and services that are web based for their clients. Federal Express supports the Federal Express Innovation laboratories and The FedEx Institute of Technology located at the University of Memphis.
	Pipeline and Hazardous Materials Safety Administration (PHMSA)	PHMSA develops regulations and standards for classifying, handling, and packaging hazardous materials across modes within the United States.	To ensure minimal threats to life, property, or the environment due to hazardous materials-related incidents, PHMSA develops regulations and standards for classifying, handling, and packaging hazardous materials across modes within the United States, and serves as the United States' "competent authority" at the United Nations on committees working to harmonize standards for hazardous materials transportation safety and security worldwide.

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
Postal and Shipping (continued)	World Customs Organization (WCO)	The WCO is an independent, inter-governmental body designed to enhance the effectiveness and efficiency of international customs administrations.	It is particularly noted for its work in areas covering the development of global standards, the simplification and harmonization of Customs procedures, trade supply chain security, the facilitation of international trade, the enhancement of Customs enforcement and compliance activities, anti-counterfeiting and piracy initiatives, public-private partnerships, integrity promotion, and sustainable global Customs capacity building programs. The WCO also maintains the international Harmonized System goods nomenclature, and administers the technical aspects of the WTO Agreements on Customs Valuation and Rules of Origin.
	Transportation Research Board (TRB)	TRB is one of six major divisions of the National Research Council— a private, nonprofit institution that is the principal operating agency of the National Academies in providing services to the government, the public, and the scientific and engineering communities.	The TRB annually engages more than 7,000 engineers, scientists, and other transportation researchers and practitioners from the public and private sectors and academia, all of whom contribute their expertise in the public interest by participating on TRB committees, panels, and task forces. The program is supported by state transportation departments, federal agencies including the component administrations of the U.S. Department of Transportation, and other organizations and individuals interested in the development of transportation.
	National Science and Technology Council's Subcommittee on Biometrics member agencies	The subcommittee advises and assists the COT, NSTC, and other coordination bodies of the Executive Office of the President on policies, procedures and plans for federally sponsored biometric and IdM activities.	The subcommittee: • Improves the latest portal access and control systems for weapons detection and personnel identification and authentication. • Develops commercial-level enhanced monitoring and interpretation systems for automated protection, intrusion prevention and detection, and surveillance. • Conducts research on advanced biometric identifiers such as DNA, facial recognition, and thermal imaging. • Merges automated surveillance and biometric systems in an intelligent learning system.
	American Trucking Associations (ATA)	ATA is the national voice for the trucking industry before Capitol Hill, regulators, the courts and the media. It is the driving force in effecting change, ensuring that the industry's interests are vigorously promoted, and improving the business climate for trucking companies.	Conducts training in the use of trucking industry assets to commit terrorism continues to be a perceived threat because of the large number of trucks carrying large quantities of hazardous and military cargo and the relatively high frequency of major security breaches (e.g., hijackings and other theft crimes) that occur in the commercial trucking industry.
	Universal Postal Union (UPU)	The UPU is a nonpolitical organization.	UPU sets the rules for international mail exchanges and makes recommendations to stimulate growth in mail volumes and improve quality of service for customers.
	NA	Private Mail Operators.	Private mail operators have been emerging that distribute large volumes of presorted mail at low costs. At present, the bulk of these operators' businesses is domestic, with limited international volume; however, with deregulation taking hold, these operators will be increasingly active on the international scene.

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
Postal and Shipping (continued)	NA	Private Express Carriers.	Outside the largest four express carriers, other firms introduce shipments into the United States in partnership with U.S.-based carriers. For example, the Global Distribution Alliance (GDA) (led by the global transportation services company ARAMEX) offers a service that will match a regional carrier to a customer anywhere in the world and then route the shipment to its destination using its network of allied carriers.
		International Public Postal Operators.	As exclusive partners of USPS, international public postal organizations transport mail by air directly to the United States or utilize third-party providers. International postal organizations are governed by a Universal Postal Union (UPU) charter, which mandates a security clearance process known as postal customs clearance. The security clearance process streamlines both inbound and outbound international mail shipments but does not apply to shipments mailed by commercial carriers and/or freight forwarders and cleared by commercial brokers, or shipments mailed commercially by international public postal operators and cleared by commercial brokers.
	Global Distribution Alliance (GDA)	GDA is a group of over 40 leading logistics and transportation providers established to connect national express service providers with one another in a cohesive solid network that provides swift and reliable services globally.	The GDA offers comprehensive tracking facilities, utilizing state of the art tracking and tracing capabilities, allowing alliance members, agents, and customers to track and trace their shipments anywhere in the world with the click of a button.
Public Health and Healthcare	Healthcare Sector Coordinating Council (HSCC)	The mission of the HSCC is to coordinate plans, policy advice, and actions to preserve and restore the critical functions of the nation's healthcare delivery system and to support effective emergency preparedness and response to all hazards, including natural and manmade disasters.	The sector is significantly interdependent with a number of sectors that have control systems security as a critical infrastructure element including energy, communications, transportation, chemical, water, information technology, and telecommunications. No sector specific control system program activities within private sector healthcare stakeholders were identified.
Government Facilities	Government Coordinating Council	Government facilities are managed primarily by government agencies that are also the security partners. Educational facilities have additional state and local partners.	The DHS US-CERT and Control Systems Security Program are referenced in the Sector Specific Plan as resources to deal with cybersecurity issues. Interdependencies with other sectors exist such as energy, communications, transportation, chemical, water, information technology, and telecommunications where private sector programs previously defined may have applicability.

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
Banking and Finance	Financial Services Sector Coordinating Council (FSSCC)	The Financial Services Sector Coordinating Council is a group of more than 30 private-sector firms and financial trade associations that works to help reinforce the financial services sector's resilience against terrorist attacks and other threats to the nation's financial infrastructure.	No specific control systems programs. The Financial Services Sector is interdependent with other critical infrastructures where control systems, communications, and information security are significant to protective measures and mitigation. The FSSCC sponsors SMART (Subject Matter Advisory Response Team) for subject matter experts of importance to the sector. The SMART Program is to assist research and development organizations (RDOs) working on critical infrastructure protection projects and programs which align with the challenges faced by the financial industry.
	Financial Services Information Sharing and Analysis Center (FS-ISAC)	On a daily basis, the FS-ISAC reaches more than 11,000 sector participants through partnership with several FSSCC members, including the American Bankers Association, and promotes information sharing between the public and private sectors.	The FS-ISAC provides sector-wide knowledge about physical and cybersecurity risks faced by the financial services sector. The FS-ISAC allows its members to receive threat and vulnerability information immediately; share vulnerabilities and information anonymously and communicate within a secure portal; access new data feeds of threat and vulnerability information; and access a wide range of user data from which users can produce their own reports and metrics. This information sharing mechanism can leverage information from other sector ISACs that may affect the financial critical infrastructure such as the IT-ISAC and MS-ISAC.
	Financial and Banking Information Infrastructure Committee (FBIIC)	The Financial and Banking Information Infrastructure Committee (FBIIC) is chartered under the President's Working Group on Financial Markets, and is charged with improving coordination and communication among financial regulators, enhancing the resiliency of the financial sector, and promoting the public/private partnership. Treasury's Assistant Secretary for Financial Institutions chairs the committee.	No specific control systems programs. The Financial Services Sector is interdependent with other critical infrastructures where control systems, communications, and information security are significant to protective measures and mitigation.
National Monuments and Icons	Primarily government driven with the Department of the Interior as the SSA	Limited concerns with control systems. Cybersecurity of some facility systems such as power and environmental controls may be impacted, but not identified as critical per the SSP.	Limited to coordination with government agencies on protection of cyber infrastructure or cross sector collaborations with Commercial and Government Facilities sectors.

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
Emergency Services	Emergency Services Sector Coordinating Council (ESSCC)	ESSCC is comprised of the International Association of Emergency Managers, the International Association of Fire Chiefs, the International Associations of the Chiefs of Police, the National Association of State EMS Officials, the National Emergency Management Association, and the National Sheriffs' Association.	These organizations have no specific control systems security programs however; the SCC recognizes control system attacks as a threat and their response to potential adverse consequences. The sector is interdependent to a number of other sectors (energy, communications, information technology, and transportation, and chemical) with these industry and trade associations involved in control systems security.
Agriculture and Food	Cyber Security and Critical Infrastructure Coordination (CSCIC)	CSCIC was established in September 2002 to address New York State's cybersecurity readiness and critical infrastructure coordination.	In focusing on the State's cyber readiness and critical infrastructure coordination needs, CSCIC addresses issues from both a cyber and physical perspective. Being cognizant of the interdependencies between cyber and physical events is crucial. One of the initial tasks of this Workgroup was to prioritize a list of critical industry sectors to determine which would be the immediate focus of the Workgroup. The Workgroup identified thirteen critical sectors and we have prioritized those thirteen sectors to initially focus our efforts as follows: chemical, education and awareness, financial and economic, food, health, public safety, telecommunications, and utilities. Executives and state agency commissioners have been identified to serve as leads for the sectors. The sectors meet monthly via conference call to share information regarding the cybersecurity status of the sector.
	California Office of Homeland Security (OHS) Agroterrorism Initiative	OHS works with the California Department of Food and Agriculture and California Department of Public Health to improve California's response to terrorist attacks against our food supply or a catastrophic disease outbreak that impacts the State's food and agricultural industry.	The program conducts a series of regional discussion based exercises to test capabilities in preparedness, response, and recovery to a disease outbreak or terrorist attack in each of California's food industries; i.e. livestock, dairy, poultry, etc. OHS conducts a series of exercises in support of California's Cyber Terrorism Initiative to assist State of California and local agencies in developing strategies for enhancing prevention, response, and recovery capabilities to defend and secure government cyberspace in California. The program: • Engages state and local government cybersecurity stakeholders to assist them in developing and testing cyber incident response plans, procedures and policies. • Works with the State Information Security Office to sponsor cyber related training for government Information Technology (IT) professionals. OHS conducts the California Large Stadium Initiative, which is a series of exercises that explore the commonalities of large stadium/mass gathering venues related to preparedness issues and assist in developing strategies for enhancing prevention, response, and recovery capabilities. The program: assists large stadiums and mass gathering venues in establishing state-wide recommended practices for security and response procedures. Assists in developing strategies for enhancing prevention, response and recovery capabilities. Provides large stadium partners with customized training including venue roles and responsibilities, mass care and shelter issues, and crisis communication.

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
Agriculture and Food (continued)	The Center for Unconventional Security Affairs (CUSA) at the University of California Irvine	CUSA addresses the security challenges of the 21st century through innovative research and education programs that integrate experts from the public and private sectors.	CUSA has pioneered a collaborative, interdisciplinary structure that draws on the best resources available from UCI, the policy community, and the public and private sectors. CUSA conducts research and provides a range of educational and public services focused on areas of concern for human and national security. CUSA is guided by an active and engaged Board of Advisors and supported by Friends of CUSA. Our activities are focused in research, education, and public service.
	Institute for Countermeasures against Agricultural Bioterrorism (ICAB)	ICAB was developed at Texas A&M University to help guard against biological agents designed to cause plant and animal disease.	The Institute is involved in developing plans to handle emergency outbreaks that may threaten the food supply, including recovery plans to accelerate a return to normality.
	National Conference of State Legislatures (NCSL)	NCSL was created to assist state legislatures in sharing information on issues of public safety, homeland security, emergency preparedness and public health.	NCSL establishes protocols for the exchange of information between the various levels of government.
	National Institute for Agricultural Security (NIAS)	NIAS was created to address homeland security issues facing agriculture, the food system and rural communities.	NIAS enhances public awareness of the role of state Agricultural Experiment Stations and Cooperative Extension Service in addressing homeland security concerns; provides a mechanism for communication and coordination with federal agencies and the private sector seeking to access the state-based agricultural research and education system; and encourages collaboration among universities, facilitating team building and capacity building of the member institutions, serving as a catalyst to bring members with special skills and capacities together so that they can compete successfully for Homeland Security projects.
	American Society of Agronomy (ASA)	The ASA is an international organization devoted to excellence in agronomic, crop, soil, and environmental science for the betterment of the world.	Since its inception, ASA has continued to evolve, modifying its educational offerings to support the changing needs of its members. Today, ASA is seen as a progressive, scientific society meeting the needs of its members through publications, recognition and awards, placement service, certification programs, meetings, and student activities.
	Crop Science Society of America (CSSA)	CSSA is a prominent international scientific society headquartered in Madison, Wisconsin.	Since its inception, CSSA has continued to evolve, modifying its educational offerings to support the changing needs of its members. Today, CSSA is seen as a progressive, scientific society meeting the needs of its members through publications, recognition and awards, placement service, certification programs, meetings, and student activities.
	National Livestock Producers Association (NLPA)	NLPA services are designed to help member marketing agencies and credit corporations become more effective and efficient for their producer-patrons.	Through member interaction, many innovative services and programs are formed and alliances cemented which are designed to provide the livestock producer many opportunities to improve the producer's bottom line. In addition, joint ventures and cooperation among the members lead to national exposure of producers' livestock through electronic marketing systems and networks of buyers and sellers.

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
Agriculture and Food (continued)	International Dairy Foods Association (IDFA)	IDFA represents the nation's dairy manufacturing and marketing industries and their suppliers. IDFA is composed of three constituent organizations: • Milk Industry Foundation (MIF) • National Cheese Institute (NCI) • International Ice Cream Association (IICA)	IDFA is committed to facilitating growth of the dairy industry by: • Providing strategic leadership to association members, government officials, customers and other audiences to promote full and open markets to maximize sales. • Leading and coordinating industry-wide consumer communications and marketing programs. • Leading and coordinating the elimination of trade barriers and opening of markets for U.S. products. • Providing proactive, effective member services in the legislative, regulatory, technical and educational arena. • Seeking the elimination of unnecessary regulations that impede member sales. • Reducing government intervention in commercial markets.
Defense Industrial Base	National Defense Industrial Association (NDIA)	NDIA provides a legal and ethical forum for the interchange of ideas between the government and the defense industry.	NDIA provides individuals from academia, government, the military services, small businesses, prime contractors, and the international community, the opportunity to network effectively with the government - industry team, keep abreast of the latest in technology developments, and address and influence issues as well as government policies critical to the health of the defense industry and the preservation of our national security.
	Center for Strategic and International Studies (CSIS)	CSIS is a bipartisan, nonprofit organization headquartered in Washington, D.C.	CSIS conducts research and analysis and develops policy initiatives that look into the future and anticipate change. CSIS provides strategic insights and policy solutions to decision makers in government, international institutions, the private sector, and civil society.
	Institute of Electrical and Electronics Engineers-United States of America (IEEE-USA)	IEEE-USA was created in 1973 to support the career and public policy interests of IEEE's U.S. members.	IEEE-USA recommends policies and implements programs specifically intended to serve and benefit the members, the profession, and the public in the United States in appropriate professional areas of economic, ethical, legislative, social and technology policy concern. The S&T program also funds research in federal, academic and industrial laboratories that focus on technologies to support future defense applications.
	Domestic Security Alliance Council (DSAC)	DSAC is a strategic partnership between the FBI and the U.S. private commercial sector.	The DSAC enhances communications and promotes the timely and effective exchange of information. It advances the FBI mission in preventing, detecting, and investigating criminal acts, particularly those affecting interstate commerce, while advancing the ability of the U.S. private sector to protect its employees, assets, and proprietary information.
	Center for Strategic Decision Research (CSDR)	CSDR is a small research institute located near Stanford University in Menlo Park, California.	For over 20 years, CSDR has presented an annual forum—presently called The International Workshop on Global Security—in major European cities. These workshops bring together political, military, industry, and academic leaders from North American, European, Asian, and African countries to discuss global security challenges on an informal and not-for-attribution basis.
	Institute for Defense and Government Advancement (IDGA)	IDGA is a nonpartisan information-based organization dedicated to the promotion of innovative ideas in public service and defense.	UDGA brings together speaker panels comprised of military and government professionals while attracting delegates with decision-making power from military, government and defense industries. It also provides breaking news and events updates via its monthly news letter, IDGA Alert.

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
Defense Industrial Base (continued)	National Classification Management Society (NCMS)	NCMS was founded in 1964 to advance the practice of Classification Management in the disciplines of industrial security, information security, government designated unclassified information, and intellectual property and to foster the highest qualities of security professionalism among its Members.	NCMS now provides professional development for its members in the field of classification management, information security, personnel security, computer security, operations security (OPSEC), facility security, and technology security. The society: • Develops and promotes education and training of members in the application of requirements of industrial security in support of the security of the United States and its allies as described in the National Industrial Security Program. • Develops and promotes education and training of members in the application of classification management principles, practices, procedures, and techniques in protecting government designated unclassified information and intellectual property in all forms. • Advances the professionalism of Members through a formal certification program recognized by government and industry. • Advances its purpose by representation and participation on U.S. government and professional security councils, committees, boards and forums and through formal comment, proposal, petition, and coordination.
	National Association of State Energy Officials (NASEO)	NASEO is a national nonprofit organization whose membership includes the governor-designated energy officials from each state and territory.	NASEO performs activities to improve the effectiveness and quality of state energy programs and policies, provide policy input and analysis, share successes among the states, and serves as a repository of information on issues of particular concern to the states and their citizens. NASEO is an instrumentality of the states and derives basic funding from the states and the federal government.
Commercial Facilities	The Instrumentation, Systems, and Automation Society (ISA)	As a leading, global, nonprofit organization, ISA is setting the standard for automation by helping over 30,000 worldwide members and other professionals solve difficult technical problems, while enhancing their leadership and personal career capabilities.	Based in Research Triangle Park, North Carolina, ISA develops standards, certifies industry professionals, provides education and training, publishes books and technical articles, and hosts the largest conference and exhibition for automation professionals in the Western Hemisphere. ISA is the founding sponsor of The Automation Federation (http://www.automationfederation.org/).
	Aerospace Industries Association (AIA)	The AIA, founded in 1919, only a few years after the birth of flight, is the premier trade association representing the nation's major aerospace and defense manufacturers.	The association concentrates on issues covering civil aviation, space and national security. The National Security Division includes a number of functional areas including defense budget and policy; workforce, industrial base, international affairs, technical operations, and the Team America Rocketry Challenge, a contest for middle and high school students. Acquisition Policy is the focal point for many initiatives associated with federal government acquisition reform activities. Acquisition Policy functional areas also include coordination of industry environmental and safety matters and activities for the supply chain through the Supplier Management Council.

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
Commercial Facilities (continued)	American Society for Industrial Security (ASIS) International	Founded in 1955, ASIS International is the largest organization for security professionals, with more than 36,000 members worldwide.	ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests, such as the ASIS Annual Seminar and Exhibits, as well as specific security topics. ASIS advocates the role and value of the security management profession to business, the media, governmental entities, and the public. By providing members and the security community with access to a full range of programs and services, and by publishing the industry's number one magazine, *Security Management* , ASIS leads the way for advanced and improved security performance.
	National Research Council Committee on Improving Cybersecurity Research	The committee is charged with developing a strategy for cybersecurity research at the start of the 21st century.	The basic underlying premise is that research can produce a better understanding of why cyberspace is as vulnerable as it is and that such research can lead to new technologies and policies and their effective implementation, making cyberspace safer and more secure.
Critical Manufacturing	Critical Manufacturing Sector Coordinating Council (SCC)	Newly created council provides representation from major manufacturers of Primary Metals, Machinery, Electrical Equipment, and Transportation and Heavy Equipment.	The Council represents the major US Primary Metals, Machinery, Electrical Equipment, and Transportation and Heavy Equipment Manufacturing.
	American Iron and Steel Institute (AISI)	AISI is an organization of steel producers that promotes steel as the material of choice and enhances competitiveness.	The Strategic Review Team recommends that Manufacturing and Technology activities be focused on areas AISI is uniquely positioned to influence. Four such areas are: Advances in safety, advances in product performance, advances in process performance, and the identification and development of disruptive technologies.
	Next-Generation Manufacturing (NGM)	NGM is a unique publication delivered to the largest and most complex firms, investing heavily in manufacturing technology, plant facilities, and supply chains. It is published four times a year.	NGM profiles the most progressive projects being undertaken by the Fortune 1000. An unparalleled group of editorial advisors and contributors make it the leading information source for corporations seeking to stay ahead of the curve. C-Level Management, Directors, IT and Operational heads read NGM to ensure they are building lean operations and making the right decisions for their company.
	American Society for Industrial Security (ASIS) International	Founded in 1955, ASIS International is the largest organization for security professionals, with more than 36,000 members worldwide.	ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests, such as the ASIS Annual Seminar and Exhibits, as well as specific security topics. ASIS advocates the role and value of the security management profession to business, the media, governmental entities, and the public. By providing members and the security community with access to a full range of programs and services, and by publishing the industry's number one magazine, Security Management, ASIS leads the way for advanced and improved security performance.

Table D-1. (continued).

Sector	Program/Organization	Description	Activity
Critical Manufacturing (continued)	National Association of Manufacturers(NAM)	The nation's oldest and largest broad-based industrial trade association, represents 14000 companies in every industrial sector in every state	NAM supports a better government-industry partnership and was a founding member of the Internet Security Alliance (ISA) to that end, co-marketing the ISA's services on the NAM Web site. In March 2004, ISA released its cyber security guide for small business, based on research with 100 companies including those of several NAM Board members, thus filling a clear need.