PROTECTING THE FEDERAL GOVERNMENT'S INFORMATION SYSTEMS AND CRITICAL INFRASTRUCTURE

Protecting the Federal Government's information systems and critical infrastructure involves both a federal-systems focus and a focus on the critical infrastructure which supports federal government information systems. The complexity and interdependency of these supporting critical systems requires risk management within the IT Sector, which builds, manages and maintains the IT infrastructure itself, and the cybersecurity of all sectors, including those affecting federal government information systems, the Defense Industrial Base, and the communications and management control systems upon which federal information systems rely.

I. Federally controlled Information Systems and Federally Controlled Systems Supporting CI

DHS Contact: Jenny Menna, National Cyber Security Division, (703-235-5316)

Scope: Protecting federal computer systems and the systems that support CI.

Overall: Develop a long-range plan to improve the effectiveness and efficiency of information security programs.

Short-Term: Within two years, for Federally controlled information systems and Federally controlled systems supporting CIKR, the Office of Management and Budget (OMB), Department of Homeland Security (DHS), National Institute of Standards and Technology, and national security authorities will work with the departments and agencies to reduce risk through better planning for and more consistent implementation of security controls and improved performance measurement of agency security programs and processes.

Focus areas

1. Increase compliance with the Federal Information Security Management Act (FISMA), Homeland Security Presidential Directive 7 (HSPD-7), and guidance concerning agency continuity of operations and national security/emergency preparedness telecommunications through:
   - Integrating requirements of FISMA, HSPD-7, Federal Emergency Management Agency (FEMA) guidance and National Communications System Directives to simplify processes and promote consistent implementation across government,
   - Continuing to define and prioritize Federally controlled information systems by risk considerations,
   - Increasing the number of information technology (IT) systems meeting key FISMA performance measures, and
   - Improving the quality of agency FISMA processes through increased qualitative assessments by agency Inspectors General (IG) and other independent experts as appropriate.

2. Promote more cost-effective implementation of key security controls through developing common security solutions.
    - Achieve greater efficiency and effectiveness through standardizing and sharing capabilities, skills, and processes across government, to the maximum extent practicable (i.e., implementing the Information Systems Security Line of Business)

Process

1. OMB to provide major initiatives and goals for each focus area.
2. OMB to identify milestones for meeting goals for initiatives identified.
3. OMB to indicate what metrics will be used to measure improved performance.
4. OMB/DHS concurrence on goals, milestones, and metrics obtained.
5. Senior leadership buy-in obtained.
6. Progress monitored with quarterly staff meetings and quarterly/semi-annual updates.
7. Quarterly and semi-annual reports prepared as applicable.

Responsible Organizations

OMB, through the Administrator, Office of E-Government and IT, is responsible for identifying the goals and overseeing the initiatives cited in this Plan, but effective execution largely depends on departments and agencies.

Goals

The goals under this Plan are to improve the protection of Federally controlled information systems and Federally controlled systems supporting CIKR using the following measures and others to be developed later to:

- Determine immediate and root causes of current information security vulnerabilities and gaps
- Provide leadership and direction for mitigating the risk from these vulnerabilities and gaps
- Implement a set of risk-informed, cost-effective controls and measures to adequately protect information and Federally controlled information systems
- Adapt to rapidly changing technologies and risk environments

Metrics and Baselines	3rd Quarter FY05 Status	2nd Quarter FY06 Status	2nd Quarter FY07 Status	2nd Quarter FY08 Status
Metric	Federal Departments and Agencies	Federal Departments and Agencies	Federal Departments and Agencies	Federal Departments and Agencies
FISMA compliance—Certification and accreditation	79% of systems certified and accredited	84% of systems certified and accredited	85% of systems certified and accredited	89% of systems certified and accredited
FISMA compliance—Certification and accreditation	IGs rate 15 agencies as having good or satisfactory processes	IGs rate 17 agencies as having good or satisfactory processes	IGs rate 17 agencies as having good or satisfactory processes	IGs rate 19 agencies as having good or satisfactory processes
FISMA compliance—Plan of action and milestone	IGs verify the process at 18 agencies to remediate IT security weaknesses	IGs verify the process at 19 agencies to remediate IT security weaknesses	IGs verify the process at 19 agencies to remediate IT security weaknesses	IGs verify the process at 19 agencies to remediate IT security weaknesses
FISMA compliance—Incident handling	Sporadic/low levels of reporting by some agencies	Sporadic/low levels of reporting by some agencies	Increased reporting by some agencies, but sporadic/low levels of reporting by other agencies persists.	Increased reporting by some agencies, but sporadic/low levels of reporting by other agencies persists.
FISMA compliance—Incident handling	Einstein incident detection tool installed by DHS/NCSD at 2 Departments and Agencies	Einstein incident detection tool installed by DHS/NCSD at 5 Departments and Agencies	Einstein incident detection tool fully installed by DHS/NCSD at 12 Departments and Agencies with 4 additional in process.	Einstein incident detection tool fully installed by DHS/NCSD at 12 Departments and Agencies with 4 additional in process.
FISMA compliance—Categorization of systems by risk impact level	Baseline data from agencies not currently available	92% of systems assigned a risk impact level	93% of systems assigned a risk impact level (From annual 2006 FISMA report)	94% of systems assigned a risk impact level
FISMA compliance—Tested contingency plans	57% of contingency plans tested on an annual basis	58% of contingency plans tested on an annual basis	73% of contingency plans tested on an annual basis	81% of contingency plans tested on an annual basis
FISMA compliance—Tested security controls	76% of systems have security controls tested on an annual basis	67% of systems have security controls tested on an annual basis	83% of systems have security controls tested on an annual basis	91% of systems have security controls tested on an annual basis

Metrics and Baselines	3rd Quarter FY05 Status	2nd Quarter FY06 Status	2nd Quarter FY07 Status	2nd Quarter FY08 Status
Metric	**Federal Departments and Agencies**	**Federal Departments and Agencies**	**Federal Departments and Agencies**	**Federal Departments and Agencies**
FISMA compliance—Agency oversight of contractor systems	IGs verify that 16 agencies have used appropriate methods to ensure that contractor provided services are adequately secure	IGs verify that 18 agencies have used appropriate methods to ensure that contractor provided services are adequately secure	IGs verify that 18 agencies have used appropriate methods to ensure that contractor provided services are adequately secure	IGs verify that 17 agencies perform oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance. [1 agency (SSA) IG answered "not applicable," and one agency IG (DoD) did not answer.]
IT systems installed and maintained in accordance with security configurations	Baseline data will be available September 15, 2005	22 agencies have an agency wide security configuration policy	22 agencies have an agency wide security configuration policy	24 agencies have an agency wide security configuration policy
Efficiency—Information Systems Security Line of Business	FY07 business case currently in development. OMB established steering group to govern implementation	DHS designated managing agency for the line of business. Staffing for the program management office is underway	Program Management Office established and approximately 85% staffed.	Program Management Office established and approximately 100% staffed.
Efficiency—Development of contracting vehicles for security hardware, software, and services	1 contracting vehicle for security training (USA Learning)	1 contracting vehicle for security training (USA Learning)	No contract vehicles developed at this time. Interagency work groups in process of evaluating agency common needs to determine priorities.	No contract vehicles developed at this time. Technical requirements for 3 security tools: configuration management, vulnerability assessment, and network mapping have been finalized and provided to GSA for procurement

Metrics and Baselines	3rd Quarter FY05 Status	2nd Quarter FY06 Status	2nd Quarter FY07 Status	2nd Quarter FY08 Status
Metric	**Federal Departments and Agencies**	**Federal Departments and Agencies**	**Federal Departments and Agencies**	**Federal Departments and Agencies**
				action under the SmartBUY program.
Efficiency—Establishment of Shared Service Centers for IT security products and services	None currently established	None currently established	3 agencies selected as SSCs for Security Awareness and Training (Office of Personnel Management, Department of State, and Department of Defense). 2 agencies selected as SSCs for FISMA Reporting. (Environmental Protection Agency and Department of Justice)	3 agencies selected as SSCs for Security Awareness and Training (Office of Personnel Management, Department of State, and Department of Defense). 2 agencies selected as SSCs for FISMA Reporting. (Environmental Protection Agency and Department of Justice)

Metrics and Fiscal Year Targets:

Metric	FY2006	FY2007	FY2008
FISMA compliance— Percentage of systems certified and accredited	90% (95% of high risk systems)	90% (100% of high risk systems)	95% (100% of high risk systems)
FISMA compliance— Agencies with good or higher certification and accreditation processes	20	22	24
FISMA compliance— Agencies with verified processes to remediate IT security weaknesses (plans of action and milestones)	20	22	24
FISMA compliance— Incident handling – agencies with automated intrusion detection tool (Einstein)	8	16	24
FISMA compliance— Categorization of systems by risk impact level	80%	100%	100%
FISMA compliance— Tested contingency plans	65% (95% of high risk systems)	80% (100% of high risk systems)	90% (100% of high risk systems)
FISMA compliance— Tested security controls	85% (95% of high risk systems)	90% (100% of high risk systems)	95% (100% of high risk systems)

Metric	FY2006	FY2007	FY2008
FISMA compliance— Agencies using appropriate methods to ensure contractor provided services are adequately secure	18	20	24
FISMA compliance— IT systems installed and maintained in accordance with security configurations	security configurations implemented for greater than 70% of the systems inventory (80% of high risk systems)	security configurations implemented for greater than 80% of the systems inventory (100% of high risk systems)	security configurations implemented for greater than 96% of the systems inventory (100% of high risk systems)
Efficiency— Number of Scorecard agencies above 90% of Certification and Accreditation, tested security controls, and tested COOPs	0 (planning phase)	0 (planning phase)	Available Q4 FY08
Efficiency— Number of scorecard agencies who report the time necessary to complete reporting or training is reduced, or they are able to redirect FTEs to other security activities when using SSCs	0 (planning phase)	0 (planning phase)	Available Q4 FY08
Efficiency— Number of agencies reporting cost savings from using FISMA reporting SSCs	0 (planning phase)	0 (planning phase)	Available Q4 FY08

Initiatives
OMB's major initiatives and the focus areas to which they contribute are shown below.

Initiative	FISMA compliance	Cost effective implementation
Information Systems Security Line of Business		X
A-11 Budget Process		X
FISMA reporting	X	
President's Management Agenda	X	

Descriptions of each one of these initiatives are attached and include a description of the initiative and responsible organization, expected outcomes, milestones, impediments/challenges, and metrics.

Methodology for Evaluation
The initiative lead is responsible for the initial assessment of the validity of the data for each of the initiatives and for tracking progress of the initiative. OMB and DHS will monitor the validity of the data as part of initiative implementation and reporting metrics as defined. Additionally, as needed independent groups (e.g., IGs, Government Accountability Office, and other experts) will validate data during planned engagements.

II. Information Systems Supporting Critical Infrastructure Beyond Federal Control

DHS Contacts: Jenny Menna, National Cyber Security Division (NCSD), (703-235-5316) for the Information Technology Sector Specific Plan; Charles H. Davis, Office of Infrastructure Protection, (703-235-3636) for the National Infrastructure Protection Plan (NIPP) Program Management Office; Brian C. Scott, Office of Infrastructure Protection, (703-235-5284) for the NIPP Metrics and Reporting Office

Scope: Protecting federal computer systems and the systems that support CI.

Overall: Develop a long-range plan to improve the effectiveness and efficiency of information security programs.

Short-Term: Federal computer systems must rely on IT and Communications infrastructure that are not within federal control. DHS the responsibility for plans and leadership that will encourage improved protection of such systems. The Department has finalized and began implementation of the June 2006 National Infrastructure Protection Plan (NIPP) and is in the process of the 2009 Triennial Review after its approval. This was followed by the approval and release of the first Information Technology (IT) Sector Specific Plan (SSP) in May 2007. Together the NIPP, IT SSP, and other 18-CI and key resource (CIKR) SSPs provide a coordinated approach for establishing national priorities, goals, and requirements for CIKR protection so that Federal funding and resources are applied in the most effective manner to reduce vulnerabilities, deter threats, and minimize the consequences of nationally significant events and other incidents. The NIPP establishes the overarching concepts relevant to all CIKR sectors identified in Homeland Security Presidential Directive 7 (HSPD-7) or by the Secretary, and addresses the physical, cyber, and human elements of the infrastructure required for effective implementation of comprehensive programs. As appendices to the NIPP, the CIKR SSPs also provide additional detail on efforts to reduce cyber risk across the 18 CIKR sectors. These plans and activities directly address information systems that support CI beyond federal control, including those that directly support the Government Facilities and the Defense Industrial Base Sectors.

Focus areas

The NIPP acknowledges that the U.S. economy and national security are highly dependent on the cyber infrastructure because it enables the Nation's essential services. The term "cyber" refers to electronic information and communications systems and the information contained therein. Although innovative technology and interconnected networks improve productivity and efficiency in operations, they also increase the Nation's risk if cyber security is not addressed and integrated appropriately. To address this risk, the NIPP includes an IT Sector responsibility, as well as a cross-sector cyber element. The IT Sector produces and provides hardware, software, and IT systems and services. NCSD serves as the Sector-Specific Agency (SSA) for the IT Sector and works closely with public and private sector security partners to identify and manage Sector risk. All CIKR sectors are consumers of IT, and as such, are responsible for implementing cyber security within and for the cyber infrastructure that they use. NCSD provides cross sector cyber security support to assist other CIKR sectors to improve the cyber security of their respective cyber infrastructure. This assistance includes contributing cyber elements to the NIPP during its annual reviews and triennial revision; delivering cyber CIKR

protection expertise to SSAs and SSP authors to help them enhance the cyber aspects of their risk management efforts; providing cyber expertise and content to various DHS risk assessment methodologies; and reviewing SSPs and Sector CIKR Protection Annual Reports (Sector Annual Reports) to ensure sectors' CIKR protection efforts address cyber assets and risks. The DHS Office of Infrastructure Protection has responsibility for overall NIPP implementation and ensuring that CIKR Sectors address the physical and human elements of their infrastructures.

The NIPP and its component SSPs, including the IT SSP, serve as the foundation for addressing the challenges to securing the Nation's critical information infrastructure. Other initiatives, including control systems security, the United States-Computer Emergency Readiness Team (US-CERT) and cyber exercises, which are described later in this document, further support the goal of ensuring the security of information systems across the CIKR sectors. Specifically, these initiatives address the GAO-identified actions for policy and guidance, trusted relationships, analysis and warning, and information sharing incentives that are discussed below.

1. **Policy and Guidance.** Develop a comprehensive and coordinated national plan to facilitate CIKR protection that clearly delineates the roles and responsibilities of Federal and nonfederal security partners, defines interim objectives and milestones, sets time frames for achieving objectives, and establishes performance measures.

2. **Trusted Relationships.** Develop productive relationships within the Federal Government and between the Federal Government and State and local governments and the private sector.

3. **Analysis and Warning Capability.** Improve the Federal Government's capabilities to analyze incident, threat, consequence, and vulnerability information obtained from numerous sources and share appropriate, timely, and useful warnings and other information concerning both cyber and physical threats to Federal and nonfederal entities.

4. **Information Sharing Incentives.** Provide appropriate incentives for nonfederal entities to increase information sharing with the Federal Government and enhance other CIKR protection efforts.

In addition, the NIPP and IT SSP address several of the GAO findings contained in GAO-05-827T "Critical Infrastructure Protection: Challenges in Addressing Cybersecurity" dated July 20, 2005, and in GAO-07-310 "High Risk Series – An Update" dated January 2007. The NIPP and IT SSP will increase awareness about cyber security roles and capabilities, facilitate effective partnerships with stakeholders, enhance analysis and warning capability, and improve two-way information sharing with these stakeholders.

Process

1. DHS to provide major initiatives and goals for each focus area.
2. DHS to identify milestones for meeting goals for initiatives identified.
3. DHS to indicate what metrics will be used to measure improved performance.
4. OMB/DHS concurrence on goals, milestones, and metrics obtained.
5. Monitor progress with monthly staff meetings and quarterly updates.
6. Quarterly status reports will be held with OMB and GAO to monitor progress.

Responsible Organizations
DHS, through the Assistant Secretary for Cybersecurity and Communications, the Director of the National Cyber Security Division, and the Assistant Secretary for Infrastructure Protection, is responsible for identifying the goals and overseeing the initiatives cited in this Plan, but effective execution is dependent on the SSA for the 18 CIKR sectors and other entities, including private sector owners and operators, to implement the initiatives and measure their results.

The IT Sector is comprised of producers of IT, focusing on hardware manufacturers, software developers, and service providers; and the Internet as a key resource. The public-private partnership embodied in the IT Sector Coordinating Council is a crucial component, as the vast majority of all CIKR is owned and operated by the private sector. An effort to implement the IT SSP began in earnest in February 2007 and through continued collaboration in 2008 with representatives of the IT SCC and the IT Government Coordinating Council (GCC) is making progress toward achieving its goals of protection and prevention through risk management, situational awareness, and response, recovery and reconstitution.

Goals
The overarching goal of the NIPP is to build a safer, more secure, and more resilient America by enhancing protection of the Nation's CIKR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency. DHS will use the following measures and others to be developed later. Current metrics are framed around process or outputs in developing plans and completing milestones. As the NIPP and IT SSP are revised over time, outcome metrics will be developed and used in place of the following process-oriented metrics.

Milestones and Baselines - FY 2008 (End of Year):

Initiative	Focus Area	Milestone	Baseline Completion Date
NIPP—18 CIKR Sectors			
Develop NIPP to serve as guiding framework for securing CIKR	Policy & Guidance, Trusted Relationships	Finalized NIPP Base Plan	Q3 FY06
Develop core metrics and sector-specific metrics for NIPP performance measurement in collaboration with security partners	Policy & Guidance, Trusted Relationships, Information Sharing Incentives	NIPP Metrics Identification	Q3 FY07 Q3 FY08 – core metrics update
Develop performance measurement levels associated with each metric in collaboration with security partners	Policy & Guidance, Trusted Relationships, Information Sharing Incentives	Performance Measurement Thresholds/Levels	Q3 FY07 Q3 FY08
Develop data collection methods in collaboration with partners	Policy & Guidance, Trusted Relationships, Information Sharing Incentives	Data Collection Methods/Tools	Q3 FY07 Q3 FY08
Identify metrics for effective security practices already in use	Policy & Guidance, Trusted	Metrics Effective Security Practices	Q1 FY07 Q1 FY08

Initiative	Focus Area	Milestone	Baseline Completion Date
by some SSAs	Relationships, Information Sharing Incentives		
Collect the necessary data to assess/measure performance of each sector	Analysis & Warning Capability	Sector CIKR Protection Annual Reports	Q4 FY06 Q4 FY07 Q4 FY08
Assess all sectors together to develop national assessment of the "state of CIKR protection"	Analysis & Warning Capability	National CIKR Protection Annual Report	Annually; completed FY06 completed FY 07 Q4 FY08
Develop updates to metrics on a regular basis	Policy & Guidance	Performance Metrics Updates	Q4 FY07 Q4 FY08
NIPP Triennial Review	Policy & Guidance, Trusted Relationships	Revised NIPP Base Plan	Q4 FY08
IT Sector			
Develop a framework and process for developing IT sector-specific metrics in collaboration with security partners	Policy & Guidance, Trusted Relationships, Information Sharing Incentives	IT Sector Metrics Framework	Q2 FY08
Develop IT sector-specific metrics in collaboration with partners	Policy & Guidance, Trusted Relationships, Information Sharing Incentives	Implementing the SSP and Tracking Progress Chapter in the IT SSP	Q3 FY08
Develop data collection and reporting processes and tools for metrics to assess progress against sector goals	Policy & Guidance, Information Sharing Incentives	Metrics procedures and protocols	Q1 FY07 (completed high level structure and reporting mechanism) Q3 FY08 (full procedures and collection guidelines)
Develop IT Sector risk assessment methodology in collaboration with security partners	Analysis & Warning Capability, Policy & Guidance, Trusted Relationships	Risk Assessment Methodology	Q1 FY07 (completed methodology framework) Q1 FY08 (full methodology) Q2 FY08 (Pilot)
Develop IT Sector Annual Report in collaboration with security partners	Trusted Relationships	IT Sector Annual Report	Q4 FY07 (completed for the 2007 report) Q4 FY08 (2008

Initiative	Focus Area	Milestone	Baseline Completion Date
			report completion date)
Identify sub-functions and elements of critical IT Sector functions in collaboration with security partners	Analysis & Warning Capability, Trusted Relationships	Critical IT Sector functions decomposition matrix	Q1 FY08
Develop measures and thresholds for consequence, vulnerability, and threat in collaboration with security partners	Analysis & Warning Capability, Trusted Relationships	Risk Measures	Q1 FY08
Identify threats to the Sector and map them against the critical IT Sector functions in collaboration with security partners	Analysis & Warning Capability, Trusted Relationships, Information Sharing Incentives	Threat and Critical Functions Mapping	Q1 FY08
Identify protective measures for nationally critical IT Sector infrastructure to mitigate threats, vulnerabilities, and consequences in collaboration with security partners	Analysis & Warning Capability, Trusted Relationships	Protective Measures Guidance	Q1 FY07 (completed identification of existing protective programs and potential capability gaps as part of IT SSP) Q3 FY08 (Identify additional protective measures based on assessments)
Coordinate IT Sector research and development (R&D) priorities and efforts	Information Sharing Incentives, Trusted Relationships	R&D Workshop	Q4 FY08 Q4 FY09 (annually)
Update IT SSP as part of annual review process in collaboration with security partners	Policy & Guidance, Trusted Relationships	Revised IT SSP	Q1 FY07 (completed first version) Q2 FY08 (annually)
Initiate Threat Intelligence Coordination Working Group (TICWG), in collaboration with the Homeland Infrastructure Threat and Risk Analysis Center and sector security partners, to enhance the quality of analytical and threat warning products targeted to the IT Sector	Information Sharing Incentives, Trusted Relationships, Analysis & Warning Capability	Establish working group Quarterly threat briefing to the sector from HITRAC and other intelligence community partners	Q4 FY07

Initiative	Focus Area	Milestone	Baseline Completion Date
Cross Sector Cyber			
Continue to provide cross-sector cyber security guidance and support to SSAs and federal agencies in their CIKR protection efforts	Policy & Guidance, Trusted Relationships	Review and provide input on cyber components of other SSPs Review and provide input on cyber components of Sector Annual Reports	Q1 FY07 (completed) Q1 FY08 (annually) Q3 FY07 (completed) Q3 FY08 (annually)
Assess cyber security trends across the CIKR sectors within the overall national assessment of the state of critical infrastructure protection activities as provided by the CIKR sectors in their Sector Annual Reports	Policy & Guidance	National CIKR Protection Annual Report and Cyber Annex to the National CIKR Protection Annual Report	Q4 FY07 Q4 FY08 (annually)
Develop an asset identification methodology for SSAs to use to determine cyber infrastructure elements	Analysis & Warning Capability, Trusted Relationships	Cyber Asset Identification Methodology	Q2 FY07 (completed) Q4 FY07 (implemented in at least one Sector)
Develop a cyber security vulnerability assessment methodology that SSAs may use as part of their Sector risk assessment approaches	Analysis & Warning Capability, Trusted Relationships	Cyber Security Vulnerability Assessment Methodology	Q1 FY07 (completed) Q2 FY08 (automated assessment)
Co-chair monthly Cross Sector Cyber Security Working Group meetings	Analysis & Warning Capability, Trusted Relationships, Information Sharing Incentives	Co-chair monthly meetings	Ongoing
Provide US-CERT portal access to CI sector partners to deliver cyber security analytic and warning products and encourage information sharing among stakeholders and with DHS to complement the Homeland Security Information Network	Analysis & Warning Capability, Trusted Relationships, Information Sharing Incentives	Launch Cross Sector Cyber Security Working Group Portal Compartment	Q4 FY07
Control Systems Security			
Develop and distribute Control Systems Cyber Security Self Assessment Tool to the control	Analysis & Warning Capability,	Control Systems Cyber Security Self Assessment Tool	Q1 FY08

systems community to qualitatively measure their cyber security posture and encourage enhanced protective efforts	Information Sharing Incentives		
Develop curriculum guidance focusing on cyber security aspects of CI control systems for incorporation into university information security degree programs	Policy & Guidance	Control Systems Security Curriculum Guidance	Q2 FY08
Assess CI control systems and provide recommendations to mitigate and address vulnerabilities to protect against cyber threats	Analysis & Warning Capability	Control Systems Assessments	Q4 FY07 (Ongoing)
Work with academia to draft curriculum guidance at the undergraduate and graduate level for incorporation into university information security degree programs, focusing on the cyber security aspects of control systems.	Policy & Guidance, Trusted Relationships	Training and Awareness Workshops	Q3FY07
Develop a set of common procurement requirements and contractual language that CIKR owners and operators can leverage to ensure the control systems they are purchasing or maintaining are operated in compliance with security requirements.	Policy & Guidance, Trusted Relationships	Cyber Security Procurement Language for Control Systems	Q2 FY08
Sponsor training and awareness workshops for domestic and international industry stakeholders and security partners to increase awareness of potential cyber incident impacts and vulnerabilities	Policy & Guidance, Trusted Relationships	Training and Awareness Workshops	Q4 FY07 (Ongoing)
Cyber Exercises			
Conduct Chicago regional tabletop exercise (TTX) with CI security partners to analyze the impact of an incident to interdependent cyber infrastructure in the region	Trusted Relationships, Analysis & Warning Capability	ChicagoFIRST TTX	Q4 FY07
Sponsor and execute cyber TTX in Oregon for TOPOFF 4 to discuss cyber impacts and response related to the TOPOFF4 exercise incident	Trusted Relationships, Analysis & Warning Capabilities, Policy	Oregon TTX	Q4 FY07

scenario	& Guidance		
Conduct National Cyber Exercise: Cyber Storm II, which focuses on four CI sectors and will include participants from six additional CI sectors	Trusted Relationships, Analysis & Warning Capability, Policy & Guidance	Cyber Storm II	Q2 FY08
US-CERT			
Deploy Einstein at thirteen Federal agencies	Trusted Relationships, Analysis, & Warning Capability	Einstein Program	Q2 FY07 (completed)
Create a Quarterly Trends and Analysis Report for public constituents and streamline the publishing process	Information Sharing Incentives, Analysis & Warning Capability	Quarterly Trends and Analysis Report	Q2 FY07 (completed) Q3 FY07 (completed) Q4 FY07 (completed) Q1 FY08 (completed) Q2 FY08 (completed) Q3 FY08 (completed) Q4 FY08
Create a web site for the Homeland Secure Data Network to facilitate the dissemination of important and SECRET classified information with constituents in the Intelligence Community	Information Sharing Incentives, Trusted Relationships, Analysis & Warning Capability	HSDN Web Site	Q3 FY07 (completed)
Redesign the public US-CERT web site to better feature and highlight the National Cybersecurity Alert System	Information Sharing Incentives, Analysis & Warning Capability	Public US-CERT Web Site	Q1FY08 (completed)
Continue to collaborate with NIST to expand the National Vulnerability Database, a US Government repository of standards based vulnerability management data.	Information Sharing Incentives, Analysis & Warning Capability	National Vulnerability Database	Q4FY08

Metrics and Fiscal Year Targets

NCSD is in the process of revising our metrics for the referenced programs to ensure they adequately address the specific focus areas and provide insight into program efficiency and results.

Initiatives

DHS's major initiatives and the focus areas to which they contribute are shown below.

Initiative	Policy & Guidance	Trusted Relationships	Analysis & Warning Capabilities	Information Sharing Incentives
NIPP	**X**	**X**	**X**	**X**
IT SSP	**X**	**X**	**X**	**X**
Cross Sector Cyber	**X**	**X**	**X**	**X**
Control Systems Security	**X**	**X**	**X**	**X**
Cyber Exercises	**X**	**X**	**X**	
US-CERT	**X**	**X**	**X**	**X**

Descriptions of each one of these initiatives are attached and include a detailed description of the initiative and responsible organization, expected outcomes, milestones, impediments/challenges, and metrics.

Methodology for Evaluation

The initiative lead is responsible for the initial assessment of the validity of the data for each of the initiatives and for tracking progress of the initiative. DHS components will establish a methodology for monitoring the validity of data as part of initiative implementation and reporting metrics as defined. Additionally, as needed independent groups (e.g., contractors, DHS Inspector General, and GAO) will validate data during planned engagements.

AREA F.1: Information Systems Security Line of Business

Focus Area: Cost effective implementation

Lead Agency: Office of Management and Budget (OMB) and Office of Cybersecurity and Communications (CS&C), National Cyber Security Division, Department of Homeland Security (DHS)

Description
Information Systems Security (ISS) was proposed as an eGov Line of Business (LOB) to provide leadership and direction for improving effectiveness and consistency of information systems security across the Federal Government. The goal of the LOB is to address those areas of information security which are common to all agencies and are not specific to the mission of any individual agency. The ultimate outcome will be substantial improvement in Federal Government information system security effectiveness and consistency, and more efficient use of resources.

Expected Outcomes
The ISS LOB will:
- Raise the level of ISS across government agencies for areas of information security that are common to all agencies and not specific to the mission of any individual agency, and to eliminate the need for each agency to develop their own duplicative capability.
- Provide benefits and cost savings/avoidance through shared services by eliminating duplication, increasing expertise through specialization, and freeing-up resources for mission specific requirements and other tailored security requirements above what is offered through the LOB. This approach is referred to as "common solutions."
- Through consolidation, establish specialized Shared Service Centers (SSC) that provide a common framework for the U.S. Government's ISS, speed remediation and implementation of enhancements, share best practices, provide expertise through consultation, and use aggregated acquisitions for products and services when appropriate.
- Establish a governance structure that elevates decision-making for common activities of ISS from "local" programs to an enterprise level that ensures consistency and strengthens ISS government-wide.
- Provide opportunities and advantages that will improve ISS for agencies that are resource constrained.

Accomplishments
- Completed guidelines for implementing the ISS LOB. (Q2FY06)
- Established the Program Management Office. (Q3FY06)
- Developed and submitted FY08 joint business case to OMB for the ISS LOB. (Q4FY06)
- Created interagency review/evaluation teams for the Training and Federal Information Security Management Act (FISMA) reporting areas. (Q4FY06)
- Created an interagency Implementation Work Group. (Q1FY07)
- Established the Federal Systems Security Governance Board (FSSGB). (Q1FY07)
- Completed review/evaluation of agency capability statements for FISMA Reporting and Security Awareness Training. (Q1FY07)
- Completed final recommendations report. (Q1FY07)

- Announced selection of SSC for Security Awareness Training and FISMA Reporting. (Q2FY07)
- Completed Customer Agency Guidelines. (Q3FY07)
- Provided template for SSC Service Level Agreement. (Q3FY07)
- Established four interagency work groups. (Q3FY07)
- Submitted FY09 Joint Business Case. (Q3FY07)
- Developed, submitted, and gained approval from FSSGB on recommendations on identifying specialized/role-based Tier II training and situational awareness, and incident response (SAIR). (Q1FY08)
- Began delivery of Tier 1 SSCs for security awareness training programs that meet FISMA requirements through the Joint Department of State-USAID Solution Team (JSAS), OPM and DoD Shared Service Center (SCC). (Q1FY08)
- Obtained responsibility for overseeing the selection criteria and implementation of the Access Providers for the Trusted Internet Connection (TIC) initiative. (Q2FY08)
- Submitted work group recommendations report to FSSGB for system certification. (Q2FY08)
- Developed technical requirements for system certification and accreditation (C&A). (Q2FY08)
- Developed draft technical requirements for Tier II Training and SAIR Tier 1. (Q2/Q3FY08)

Milestones

Q4FY08

- Submit FY10 Joint business case.

FY09

- Issue request for SCO for Security Awareness Training (New submissions).
- Review/reprogram. Based on established performance measures, and current schedule and costs, review program progress and determine need to reprogram as necessary.
- Conduct review/analysis of common requirements.
- Submit FY11 Joint business case.

FY10

- Conduct review/analysis of common requirements.
- Submit FY12 Joint business case.

FY11

- Review/reprogram. Based on established performance measures, and current schedule and costs, review program progress and determine need to reprogram as necessary
- Submit FY13 Joint business case (as necessary).

FY12

- Review/reprogram. Based on established performance measures, and current schedule and costs, review program progress and determine need to reprogram as necessary.
- Submit FY14 Joint business case (as necessary).

FY13

- Conduct review/analysis of common requirements.

Impediments/Challenges

None

Metrics
NCSD is in the process of revising our program-level metrics for the referenced program to ensure they adequately address the specific focus areas and provide insight into program efficiency and results.

Remarks
Through the identification of common requirements and implementation of the ISS LOB via SSCs, the security of Federal information systems will be improved, ensuring the reliability, availability, and confidentiality of critical information systems.

The Federal Chief Information Officer (CIO) Council provides a standing forum for vetting ISS issues, and is the principal body in which the ISS LOB seeks cooperation and support. As the governance body of the ISS LOB, the FSSGB may consult with the CIO Council on key decisions affecting ISS within the Federal enterprise. The monthly CIO Council meeting is a key venue for DHS leadership to engage the community on urgent/current issues which the ISS LOB could address through interagency work groups.

As the principal provider of security tools and services, the private sector has a key interest in ISS LOB activities. The private sector must be assured that their interests are considered in deliberations, planning, and implementation of ISS LOB activities. Most public venues involving the security tools/services community provide an opportunity to assure these key stakeholders that the ISS LOB considers them vital partners in the acquisition and delivery of services to the Federal departments and agencies.

AREA F.2: National Infrastructure Protection Plan

Focus Area: Policy and Guidance, Trusted Relationships, Analysis and Warning Capabilities, Information Sharing Incentives

Lead Agency: Office of Infrastructure Protection, Department of Homeland Security (DHS)

Description
Homeland Security Presidential Directive-7 (HSPD-7) mandated development of a National Infrastructure Protection Plan (NIPP) as the primary vehicle to guide implementation of the United States' policy for enhancing protection of the Nation's critical infrastructure and key resources (CIKR). DHS is charged with developing and implementing the NIPP, which was published in June 2006.

The NIPP provides the coordinated approach for establishing national priorities, goals, and requirements for CIKR protection so that Federal funding and resources are applied in the most effective manner to reduce vulnerabilities, deter threats, and minimize the consequences of nationally significant events and other incidents. It establishes the overarching concepts relevant to all CIKR sectors identified in HSPD-7 or by the Secretary, including the Information Technology Sector, and addresses the physical, cyber, and human elements of the infrastructure required for effective implementation of comprehensive protection programs for all 18 CIKR sectors. The NIPP specifies the key initiatives, milestones, and metrics required to protect the Nation's CIKR. It sets forth a comprehensive risk management framework and clearly defines roles and responsibilities for DHS; Federal Sector-Specific Agencies (SSA); other Federal, State, local, tribal, and international entities; and private sector infrastructure owners and operators.

Expected Outcomes
- Effective allocation of CIKR protection resources to address greatest risks and gaps.
- Robust two-way information sharing between the government and the private sector.
- Voluntary participation of owners and operators.
- Improved trusted relationships between government and private industry.

Accomplishments
- Established Critical Infrastructure Partnership Advisory Council (CIPAC). (Q2FY06) held annual plenary meeting in Q4 2007 and Q4 2008
- Issued final NIPP Base Plan. (Q3FY06)
- Submitted first National CIKR Protection Annual Report. (Q1FY07) also the second in Q1FY08
- Developed NIPP core metrics for NIPP performance measurement in collaboration with security partners. (Q3FY07)
- Released 17 Sector-Specific Plans. (Q3FY07)
- Aggregated the 17 Sector CIKR Protection Annual Reports and the State and local CIKR protection submissions and develop the 2007 National CIKR Protection Annual Report; which was submitted to the executive Office of the President. (Q4FY07)
- Initiated data collection methods for collaboration with partners through the Sector Partnership Metrics framework. (Q1FY08)
- Established 18th sector in 2008 for Critical Manufacturing.

Milestones
Q3FY08
- Develop sector-specific metrics in collaboration with security partners.
- Identify metrics for effective security practices in use by sectors/SSAs.
- Collect core metrics data.
- Receive 2008 Sector CIKR Protection Annual Reports.

Q4FY08
- Assess all sectors together to develop national assessment of the state of CIKR protection through the National CIKR Protection Annual Report.
- Prepare the 2008 National Annual Report for submission to the Executive Office of the President on September 1, 2008.

Impediments/Challenges
- Coordination and collaboration with broad range of security partners.
- Voluntary participation of private sector.
- Policy barriers/impediments to information collection.

Metrics
Measure the efficacy of risk management activities performed under the NIPP and the progress made in reducing the risks of the Nation's CIKR to terrorist attack and other hazards so as to inform national and sector-level risk management decisions.

- Provide a point of reference for individual CIKR sectors to reflect their distinctive characteristics and requirements;
- Provide a basis for establishing accountability, documenting performance, identifying issues, promoting effective management, and reassessing goals and objectives; and
- Measure the effectiveness of the framework for CIKR protection public-private partnerships and gauge the success of the national partnership model in contributing to enhanced risk management and CIKR protection.

Remarks
The NIPP framework requires cyber to be included as a critical element in all 1817 existing CIKR SSPs.

AREA F.3: Information Technology Sector-Specific Plan

Focus Area: Policy and Guidance, Trusted Relationships, Analysis and Warning Capabilities, Information Sharing Incentives

Lead Agency: Office of Cybersecurity and Communications, National Cyber Security Division, Department of Homeland Security (DHS)

Description

The National Infrastructure Protection Plan (NIPP) was developed in response to Homeland Security Presidential Directive 7 (HSPD-7) to provide a consistent, unifying structure for integrating current and future critical infrastructure and key resource (CIKR) protection efforts. The Information Technology (IT) Sector-Specific Plan (SSP) is one of 18 SSPs that were published in May 2007 as appendices to the NIPP. The IT SSP provides a framework for identifying and managing Sector risk, enhancing information sharing, identifying existing and future protective programs, structuring research and development priorities, and tracking plan implementation progress.

Expected Outcomes

- Effective public-private partnership to manage risk to the IT Sector and promote overall security and resilience of the sector.
- Assessment of the risk to critical IT Sector functions and an overall risk profile for the sector.
- Identification of future protective program needs and research and development (R&D) priorities.
- Enhanced information sharing framework for the sector.

Accomplishments

- Cataloged IT Sector protective measures for nationally critical IT Sector infrastructure to mitigate threats, vulnerabilities, and consequences. (Q1FY07)
- Developed, in partnership with the IT Sector Coordinating Council (SCC) and IT Government Coordinating Council (GCC), the first joint public-private sector IT SSP. (Q1FY07)
- Met with the IT SCC regularly to develop the IT SSP and begin implementation of the actions contained therein. (Q1FY07 –Q3FY08)
- Developed core and programmatic IT Sector metrics. (Q1FY07, Q1FY08)
- Established IT SSP implementation groups comprised of SCC and GCC representatives (Q2FY07)
- Identified critical IT Sector functions. (Q2FY07)
- Developed IT Sector Annual Report. (Q3FY07, Q3FY08)
- Developed quarterly implementation schedule and work breakdown structure for IT SSP action items (Q3FY07)
- Convened Threat Intelligence Coordination Working Group (TICWG) with Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) and sector security partners to ensure the incorporation of cyber security expertise into products and briefings and facilitated the dissemination of high quality analytical and threat/warning products to IT Sector and other CIKR sector cyber stakeholders. (Q4FY07)

- Provided classified briefings to cleared IT Sector stakeholders on a broad spectrum of threats to the IT infrastructure in collaboration with HITRAC and other intelligence community partners. (Q4FY07, Q1FY08, Q2FY08)
- Identified critical IT sector sub-functions and elements of those sub-functions to prepare to identify and assess vulnerabilities and risks to these critical functions. (Q4FY07)
- Developed consequence assessment framework for the sector. (Q4FY07)
- Developed measures and thresholds for consequence, vulnerability, and threat. (Q1FY08)
- Identified threats to the sector and mapped them against the critical IT Sector functions. (Q1FY08)
- Completed the IT Sector risk assessment methodology. (Q1FY08)
- Provided IT Sector perspective to DHS pandemic influenza contingency planning efforts by adding content to DHS documentation. (Q1FY08); conducted pandemic preparedness webinar (Q3FY08)
- Developed IT Sector programmatic metrics responses. (Q2FY08)
- Initiated IT Sector Risk Assessment Pilot. (Q2 FY08)
- Conducted pilot IT Sector risk assessment for two critical functions (identify and assess vulnerabilities, threats, and consequences). (Q2FY08).
- Developed 2008 IT SSP Update. (Q3FY08)
- Evaluated IT Sector risk assessment pilot results. (Q3FY08)
- Chaired quarterly IT GCC meeting to ensure the coordination and input of IT GCC perspectives and activities with the activities stated above. (Q3FY08)

Milestones

Q4FY08

- Begin the full IT Sector risk assessment.
- Identify additional protective measures for nationally critical IT sector infrastructure.
- Chair quarterly IT GCC meeting and ensure the coordination and input of IT GCC perspectives and activities with the SCC activities stated above.

FY09

- Complete IT sector baseline risk assessment.
- Develop IT Sector Annual Report.
- Align protective programs and research and development initiatives with risks identified in the risk assessment.
- Develop and implement mitigation strategies for identified risks.
- Continuing SSP action item implementation via the SCC and GCC.

Impediments/Challenges

- Protected Critical Infrastructure Information (PCII) Concerns. PCII is an information protection tool that facilitates information sharing between the Government and the private sector; however, the private sector has continued to express concerns about the PCII Program. While the Department is confident in the PCII protections, to bolster private sector support for the program, the DHS PCII Program Office has already implemented enhancements in its operating procedures and continues to address sector concerns. In an attempt to simplify the process, US-CERT has developed an option for the private sector to submit data for PCII protection through the US-CERT Portal. Some of the IT Sector's concerns may also be addressed as they engage in the National Cyber Exercise, Cyber Storm II, which plans to use PCII to share information during the planning process.

- Inconsistency between "Top-Down" and "Bottom-Up" Risk Management Approaches. The IT Sector has voiced concern that asset-based initiatives, such as DHS Tier 1 and Tier 2 and National Asset Database (NADB) programs seem to be incompatible with the top-down, function-based approach outlined in the IT SSP. This top-down approach, which focuses on understanding the functions of the infrastructure rather than cataloging physical fixed assets, was determined to be more effective for the highly distributed IT infrastructure. The IT Sector's risk approach fulfills the intent of the NIPP Risk Management Framework by adapting and modifying its activities and concepts to address the unique IT Sector risk environment. NCSD has been working to reconcile these approaches and map examples of physical assets categories that support IT critical functions in order to facilitate response to near-term DHS data collection needs. The IT Sector will continue working with DHS and other security partners to increase awareness and understanding of its function-based approach and demonstrate how risk can be addressed through implementation of their top-down approach.
- Threat Information Sharing. The intelligence community has identified threats and countermeasures that can help the IT Sector and homeland security community implement preventive and protective measures. To ensure sensitive threat information is protected, but also shared with proper IT Sector security partners so that they can take appropriate protective actions, NCSD is identifying cleared individuals in the private and public sectors and arranging classified spaces for information sharing. The IT Sector is implementing the actions from the information sharing chapter of the IT SSP which should help to clarify and facilitate the policies, processes, and technology issues constraining the sharing of threat information at the classified and For Official Use Only (FOUO) levels. For example, the IT Sector has formed a small working group to engage with HITRAC and other intelligence community partners to share current threat information with cleared individuals, shape future analytical, threat/warning products, and develop processes to share information efficiently and effectively with those "who need to know" in order to take protective actions.

Metrics
NCSD is in the process of revising our metrics for the referenced program to ensure they adequately address the specific focus areas and provide insight into program efficiency and results.

Remarks
The IT Sector is comprised of producers of IT, focusing on hardware manufacturers, software developers, and service providers; and the Internet as a key resource. The public-private partnership embodied in the IT SCC is a crucial component, as the vast majority of all CIKR is owned and operated by the private sector.

An effort to implement the IT SSP began in earnest in February 2007 and has continued through collaboration with representatives of the IT SCC and the IT GCC over 2007 and 2008, as the IT Sector is making progress toward achieving its goals of protection and prevention through risk management, situational awareness, and response, recovery and reconstitution.

AREA F.4: Cross Sector Cyber Security

Focus Area: Policy and Guidance, Trusted Relationships, Information Sharing Incentives

Lead Agency: Office of Cybersecurity and Communications (CS&C), National Cyber Security Division (NCSD), Department of Homeland Security (DHS)

Description
All critical infrastructure and key resource (CIKR)(CI) sectors are consumers of information technology (IT), and as such, are responsible for implementing cyber security within and for the cyber infrastructure that they use. The NCSD Critical Infrastructure Protection Cyber Security Program's Cross Sector Cyber Security initiative is assisting Sector-Specific Agencies (SSAs) and other security partners with improving the security of their respective CI and key resource (CIKR) cyber infrastructure. The Cross Sector Cyber Security program provides cyber guidance and methodologies to sectors to assist them in mitigating cyber risk (especially cyber infrastructure vulnerabilities) and in developing effective and appropriate protective measures. This guidance includes contributing cyber elements to the National Infrastructure Protection Plan (NIPP); delivering cyber CIKR protection expertise to SSAs and Sector-Specific Plan (SSP) authors to help them enhance the cyber aspects of their risk management efforts; providing cyber expertise and content to various sectors' risk assessment methodologies; and reviewing SSPs and Sector Annual Reports to ensure sectors' CIKR protection efforts address cyber assets and risks.

Expected Outcomes
- Identification of systemic cyber risks and mitigation strategies for the Nation's CIKR sectors.
- Greater understanding of infrastructure interdependencies and improved security of cyber and communications assets, systems, networks, and functions.

Accomplishments
- Provided guidance documents, technical assistance, and feedback to SSAs on the development of cyber security concepts and methodologies in their SSPs. (Q1FY07)
- Developed and refined cross sector risk guidance and methodologies (e.g., cyber security vulnerability assessment (CSVA), asset identification methodology) and provided cyber security content for risk and vulnerability assessment methodologies within the Risk Analysis and Management for Critical Asset Protection (RAMCAP),), the Chemical Sector Comprehensive Review, and the Chemical Security Assessment Tool. (Q1FY07)
- Collaborated with the Intelligence Community (IC) and the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) to assess risk across sectors. (Q2FY07)
- Analyzed and commented on cyber components of Sector Annual Reports. (Q3FY07)
- Identified cross-sector cyber security research and development (R&D) requirements from across the SSPs and provided them for incorporation into the DHS Science and Technology Directorate's R&D efforts. (Q3FY07)
- Established the Cross Sector Cyber Security Working Group (CSCSWG) to address cross sector cyber risk assessment and interdependencies. The CSCSWG serves as a forum to bring government and the private sector together to address common cyber security challenges and opportunities across the CIKR sectors. Convened group and held first meeting. (Q3FY07). Meet monthly (Ongoing)
- Provided analysis of cyber components of other CIKR sectors' Annual CIKR Protection Reports to NIPP Program Management Office. (Q4FY07)

- Developed Cyber Appendix to the National CIKR Protection Annual Report. (Q4FY07)
- Coordinated a cyber security threat briefing for the NIPP Federal Senior Leadership Council and Private Sector Cross Sector Coordinating Council to ensure that stakeholders in all sectors understood the cyber threat. (Q4FY07)
- Refined cross sector risk guidance and methodologies (e.g., cyber security vulnerability assessment and asset identification methodologies) and provided cyber security content and training for risk and vulnerability assessment methodologies to the following CIKR sectors: Chemical, Communications, Government Facilities, Dams, Water, and Transportation. (Q1FY08)
- Provided a baseline analysis of cyber component of the 17177 CIKR SSPs to support the CSCSWG effort to assess cyber security in the SSPs, identify trends, interdependencies, and model practices. (Q1FY08)
- Provided input questions to the Office of Infrastructure Protection's (OIP) Protective Security Coordination Division's Enhanced Critical Infrastructure Protection (ECIP) initiative, leveraging the CSVA for Tier 1/Tier 2 asset assessments. (Q2FY08)
- Supported development of the 2008 SHIRA with HITRAC. (Q2FY08)
- Provided guidance, review and comment on cyber components of Sector Annual Reports.
- Supported CSCSWG activities related to systemic risk to the cyber infrastructure of all 18 CIKR sectors. (Q3FY08)
- Participated in writing team for 2008 National Annual Report (Q3FY08, Q4FY08)
- Briefed new Critical Manufacturing sector on cyber programs (Q308)

Milestones

Q4FY08

- Refine cross sector risk guidance and methodologies (e.g., cyber security vulnerability assessment and asset identification methodologies) and provide cyber security content for risk and vulnerability assessment methodologies.
- Analyze cyber content of the first revisions of the SSPs.

FY09

- Support cross sector cyber risk assessment process in partnership with HITRAC.
- Continue to promote use of CSVA across the sectors and enhance functionality based on user feedback.
- Participate in the Writing Team for the 2009 National Annual Report.
- Continue to provide cross sector cyber security subject matter expertise, guidance, tools and support to the 18 CIKR sectors.
- Enhance information sharing and address cross sector cyber security projects via the CSCSWG.

Impediments/Challenges

- Coordination across 18 CIKR sectors to identify common trends and systemic risks is dependent on collaboration and consensus-building within each sector (i.e. public-private sector partners as well as SSAs) and with NCSD.
- Global nature of cyber infrastructure and IT Sector will require coordination beyond the U.S.

Metrics
NCSD is in the process of revising our program-level metrics for the referenced program to ensure they adequately address the specific focus areas and provide insight into program efficiency and results.

Remarks
CS&C's National Cyber Security Division (NCSD) works in collaboration within government and with private sector owners and operators to reduce cyber vulnerabilities to critical infrastructure through the risk management framework established by the NIPP.

NCSD assists the critical infrastructure sectors in reducing the Nation's risk through integrating cyber content and guidance into vulnerability assessments and risk management programs.

DHS has developed a customizable, scalable methodology for use by sectors and their members to identify consequential cyber assets. DHS has also developed a flexible assessment tool that analyzes an entity's cyber security posture, and describes gaps and targeted considerations that can reduce overall cyber risks. This assessment tool has been leveraged in existing DHS risk and vulnerability assessment methodologies, including the RAMCAP[1] and Comprehensive Review program.[2] DHS also has been working closely with the Chemical, Dams, Drinking Water and Water Treatment Systems, Government Facilities, and Transportation Systems sectors to assess cyber security through their respective risk assessment approaches and plans to work with other sectors in the future.

DHS requested that the Critical Infrastructure Partnership Advisory Council (CIPAC) establish the CSCSWG comprising representatives of the 17 then-existing CIKR sectors with cyber security expertise. The CSCSWG held its inaugural meeting on May 30, 2007, and is designed to provide a forum and mechanism for exchanging information on common cyber security challenges and issues and addressing interdependencies. All sectors are actively participating.

[1] RAMCAP is a DHS self-assessment tool for determining vulnerability and consequences.
[2] The Comprehensive Review program is a DHS-initiated effort to assess the security posture of high-consequence CIKR.

AREA F.5: Control Systems Security

Focus Area: Policy and Guidance, Trusted Relationships, Analysis and Warning Capabilities, Information Sharing Incentives

Lead Agency: Office of Cybersecurity and Communications, National Cyber Security Division (NCSD), Department of Homeland Security (DHS)

Description
DHS' Control Systems Security Program (CSSP) coordinates efforts among government organizations, as well as asset owners, operators and vendors, to address the risk associated with Industrial Control Systems (ICS) and the associate hardware and software applications. To reduce the severity of impact of a cyber attack against ICS and to ensure resilience in design and operation, the program engages and promotes various risk identification and mitigation activities.

Expected Outcomes
CSSP was established by NCSD to increase the resilience of control systems by identifying cyber security vulnerabilities, developing vulnerability mitigation recommendations and strategies, and coordinating government and industry activities for improving the security posture within the Nation's critical infrastructure. The goal of the CSSP is to guide a cohesive effort between government and industry to reduce the risk to critical infrastructure and key resource (CIKR) industrial control systems.

Accomplishments
- Published the Procurement Language for Control Systems Security, which provides guidance to industry on improving cyber security procurement language. (Q3FY08)
- Hosted monthly teleconference meetings with control systems vendors to provide a forum to share information and common concerns, and to discuss control system security needs for legacy and next generation products. (Q1FY08, Q2FY08, Q3FY08, Q4FY08)
- Coordinated with security partners (e.g., Federal departments and agencies, Sector Coordinating Councils (SCCs), etc.) to identify vulnerabilities and develop and initiate mitigation plans for asset owners and operators of CIKR. Conducted outreach to international partners and control systems vendors to raise awareness about vulnerabilities and mitigations. (Q1FY08, Q2FY08, Q3FY08, Q4FY08)
- Performed cyber vulnerability assessments on vendor control systems and provided solutions to vulnerabilities and recommendations to protect against cyber threats. (Q1FY08, Q2FY08, Q3FY08, Q4FY08)
- Supported the United States Computer Emergency Readiness Team (US-CERT) by providing a control systems analyst and working directly with the control systems community to secure control systems through the production and dissemination of timely situational awareness information for control systems security and through the identification, analysis, and reduction of risk to control systems. (Q1FY08, Q2FY08, Q3FY08, Q4FY08)
- Sponsored training and awareness workshops with industry to increase awareness among control systems owners and operators of potential cyber incident impacts and vulnerabilities. The CSSP conducted a week long, advanced control systems cyber security workshop aimed at increasing international (United States, United Kingdom, Canada, Australia, and New Zealand) cooperation and coordination in control system cyber security. (Q3FY08)

- Delivered the Control Systems Cyber Security Self Assessment Tool (CS2SAT) for use by the control systems community to qualitatively measure the cyber security posture of their control systems environment. Negotiated additional licenses for the private sector in order to provide greater distribution of the tool. (Q1FY08, Q2FY08, Q3FY08, Q4FY08)
- Published curriculum guidance at the graduate level for incorporation into university information security degree programs, focusing on the cyber security aspects of control systems. (Q2FY08)
- Published the Federal Coordination Strategy for Securing Control Systems. (Q3FY08)
- Conducted the initial baseline review for an overall Coordinating Strategy for Securing Control Systems, leveraging the Federal Strategy and industry partnerships. (Q3FY08)
- Developed test scenarios and tested prevalent control systems vendor products for vulnerabilities and work with vendors to develop mitigations. (Q1FY08, Q2FY08, Q3FY08, Q4FY08)
- Coordinated with ISA to finalize distribution agreement for the Control Systems Cyber Security Self-Assessment Tool (CS2SAT). (Q1FY08)
- Released the Catalog of Control Systems Security Requirements in collaboration with international standards organizations. (Q2FY08)
- Delivered an "OPSEC for Control Systems" web based course that introduces the basic concepts of operations security (OPSEC) and applies these concepts to the control system environment. Course received 1st place for electronic media from the Interagency OPSEC Support Staff. (Q2FY08)
- Conducted with PCSF and the SANS Institute the 2008 SANS SCADA Summit. (Q2FY08)

Milestones

Q4FY08

- Pilot and test rapid-response program to train control systems experts on forensics and provide tools needed to equip an incident response team to support control systems security events.
- Complete the operational phase of a control systems malware identification capability.
- Distribute updated scenario and analysis for cyber attack on control systems.
- Publish a final version of the Procurement Language for Control Systems Security, which provides guidance to industry on improving cyber security procurement language.
- Design and run a pilot effort through the PCII Program where control systems vendors can submit location information on what control systems reside in which CI/KR sectors.

FY09 Milestones

- Continue training programs for security partners.
- Enhance risk reduction tools and products, including the Control Systems Cyber Security Self Assessment Tool (CS2SAT)
- Conduct vulnerability discovery, characterization, and assessments
- Perform Operational Risk Management (e.g. incident response, malware persistence and analysis)
- Finalize the Strategy for Securing Control Systems (GAO recommendation)
- Continue CIKR education efforts and planning support
- Develop products and tools for additional sectors and standards
- Support control systems field assessments (with IPD, PSAs, etc.)
- Expand Control Systems Analysis Center (recapitalization) (NDA issues)

- Expand vulnerability, validation and malware testing
- Expand advanced training for process control systems engineers
- Enhance Operational Risk Management capabilities

Impediments/Challenges
Critical infrastructure owners and operators are often reluctant to share facility and incident data, including specific security vulnerabilities and concerns, with the Federal Government. The CSSP is working closely with the private sector through the development of the Strategy to Secure Control Systems, Individual Sector Roadmaps for Securing Control Systems, Education and training, and workshop sessions to develop scenarios and processes to exchange vulnerability information and create mitigation plans. This consensus building approach to vulnerability identification and mitigation will help improve security because critical infrastructure owners and operators will be able to implement cyber security solutions based on the shared mitigation plans.

Metrics
NCSD is in the process of revising our program-level metrics for the referenced program to ensure they adequately address the specific focus areas and provide insight into program efficiency and results.

Remarks
CSSP supports the critical infrastructure and key resource sectors in reducing the Nation's vulnerability to terrorism and other disasters by providing informational products and education and training materials that assist control systems stakeholders with identifying and reducing direct risks for control systems. For example, CSSP developed a Control Systems Cyber Security Self Assessment Tool for asset owners and operators to identify control systems security vulnerabilities and solutions that can be implemented in their specific facility.

As the DHS focal point for cyber security activities related to control systems, NCSD communicates and collaborates with many diverse organizations, including government agencies, industry associations, national laboratories, equipment vendors and asset owners and operators.

AREA F.6: Cyber Exercises

Focus Area: Policy and Guidance, Trusted Relationships, Analysis and Warning Capabilities, Information Sharing Incentives

Lead Agency: Office of Cybersecurity and Communications, National Cyber Security Division (NCSD), Department of Homeland Security (DHS)

Description

The Cyber Exercises program plans, coordinates, and conducts cyber-focused exercises in order to develop, evaluate, improve, and refine the capabilities of the Department of Homeland Security (DHS) and the full spectrum of state, local, regional, international, and private sector cyber partners to prevent, protect, respond to and recover from incidents affecting cyber components (information, hardware, software, data, and networks) of the Nation's critical infrastructure. Through participation in and sponsorship of different types of exercises - workshops, tabletop, functional, and full-scale - NCSD establishes partnerships and cooperation mechanisms for information sharing with other government entities (local, state, federal, and international), as well as the private sector.

Expected Outcomes

- Planning, coordination, and execution of cyber exercises at the national/international, state, local, regional, and sector level
- Development, evaluation, improvement and refinement of DHS capabilities to prevent, protect, respond to and recover from incidents affecting cyber components of the Nation's critical infrastructure and key resource (CIKR) sectors.
- Establishment and strengthening of partnerships and cooperation mechanisms for information sharing with other government entities and the private sector through the exercise planning and execution process
- Informing of the DHS policy process to enhance DHS authorities to better execute its cyber security mission.
- Increased cyber security awareness within the U.S. CIKR sectors.
- Contribute to deterrence of cyber attacks by continually exercising and improving DHS and partners' cyber security preparedness and response capabilities.

Accomplishments

- Co-sponsored execution of the Multi-State Information Sharing and Analysis Center cyber TTX. (Q3FY05, Q3FY07)
- Planned and coordinated participation by NCSD and the NCRCG in government-wide Exercise Pinnacle [Continuity of Operations exercise]. (Q3FY05, Q3FY07)
- Co-sponsored the National Collegiate Cyber Defense Competition to foster education and growth of professionals in the cyber field. (Q3FY06, Q3FY07)
- Sponsored regional exercise (Cyber Tempest) in New York with the New York State Office of Cyber Security and Critical Infrastructure Coordination. (Q1FY07)
- Assisted the State of Delaware in conducting their annual cyber exercise by providing cyber and exercise subject matter expertise. (Q1FY07)
- Initiated planning for Cyber Storm II, including conducting the Concept Development Conference and Initial Planning Conference. (Q1FY07)

- Initiated planning and coordination efforts with the DHS Federal Emergency Management Agency (FEMA) and each of the Top Officials 4 (T4) exercise venues to include cyber in their exercise efforts. (Q1FY07)
- Sponsored and conducted cyber TTX for the Usual 5 to finalize their current draft Standard Operating Procedures in continued preparation for Cyber Storm II. (Q2FY07)
- Sponsored, coordinated, and executed a cyber workshop/ TTX in Guam for the T4 Exercise in close collaboration with the DHS FEMA. (Q3FY07)
- Initiated planning for regional TTXs in Chicago with ChicagoFIRST by conducting an Initial Planning Conference. (Q3FY07)
- Co-sponsored execution of Chicago Regional infrastructure interdependencies TTX. (Q4FY07)
- Sponsored, coordinated, and executed a cyber workshop/ TTX in Oregon for the T4 Exercise in close collaboration with the DHS FEMA. (Q4FY07)
- Planned and coordinated NCSD and Usual 5 participation in Zenith Global 07 exercise. (Q4FY07)
- Conducted Cyber Storm II Mid-Planning Conference with federal, international, state, and private sector stakeholders. (Q4FY07)
- Assisted the State of Illinois in conducting their annual functional exercise by providing cyber and exercise subject matter expertise. (Q4FY07)
- Sponsored, planned, and executed tabletop cyber exercise with State of Vermont (Q4 FY07)
- Coordinated with the DHS Science and Technology Directorate (S&T) on the testing and deployment of the Exercise Modeling Tool (CyberSMART)
- Sponsored, planned, and coordinated appropriate cyber security scenario content in the T4 Full Scale Exercise through the Cyber Working Group and in close collaboration with G&T. (Q1FY08)
- Executed Cyber Storm II national cyber exercise. (Q2FY08)
- Conducted After Action Process and developed After Action Report for Cyber Storm II exercise (Q3 FY08)
- Sponsored, planned, and executed cyber exercise with State of Massachusetts (Q4 FY08)
- Assisting ChicagoFIRST (financial services sector coordinating group) with the development and ultimate execution of a cyber exercise (execution planned for Q4 FY08)

Milestones

FY 2009

- Initiate and execute planning process for Cyber Storm III (planned for 2010). Cyber Storm planning process is historically between 18 – 24 months.
- Integrate aspects of Comprehensive National Cyber Initiative into Cyber Storm III planning and development
- Develop and deploy Cyber Exercise Program technical assistance/cyber exercise support program. This program is being developed to bolster CEP's role in supporting and participating in cyber exercises with the full range of critical infrastructure partners, (state, local, regional, sector) and to enhance collective cyber security preparedness, and to identify and address interdependencies in cyber preparedness and response
- Continue to sponsor, coordinate, and execute State, local, regional, and sector cyber exercises at an increased rate using the CEP technical assistance/cyber exercise support program
- Publish and disseminate the Cyber Storm II After Action Report

- Develop findings, identify areas for improvement, and formulate a roadmap based on the observations laid out in the Cyber Storm II After Action Report.
- Encourage action across stakeholder community to address Cyber Storm II findings as appropriate
- Participate in all phases of development, planning, and execution of National Level Exercise -09 (NLE 09)
- Coordinate with relevant sector coordination bodies to integrate Cyber objectives and play into NLE-09, and other exercises, cyber and otherwise
- Continue to coordinate and execute future Top Officials exercises.
- Continue to develop and execute an exercise plan to facilitate operational interaction with the Usual 5.
- Continue to provide technical exercise assistance to Usual 5 countries.
- Work with the International Watch and Warning Network (IWWN) to integrate capabilities into future cyber exercise plans
- Support National Cyber Response Coordination Group (NCRCG) efforts to conduct tabletop and other exercises
- Manage Cooperative Agreement with University of Texas at San Antonio (UTSA) Center for Infrastructure Assurance and Security (CIAS) to conduct state and local cyber security preparedness assessments and exercise activities

Impediments/Challenges
None

Metrics
NCSD is in the process of revising our program-level metrics for the referenced program to ensure they adequately address the specific focus areas and provide insight into program efficiency and results.

Remarks
Exercises are an important opportunity to further explore vulnerabilities of CIKR sectors, relationships, and information sharing mechanisms in a controlled environment. Once vulnerabilities have been identified, stakeholders can explore the interdependencies across the CIKR sectors and discuss/validate protective measures to combat these vulnerabilities.

Exercises allow stakeholders/participants to improve coordination and communication paths with their State, Federal, and international counterparts as well as with the private sector. Exercises are also an important component of the mechanisms that facilitate better understanding of and preparation for a variety of cyber focused scenarios that involve significant disruption of the Nation's CIKR sectors with major implications for homeland security.

In an effort to bring together and coordinate with all parties involved in securing the Nation's CIKR, including Federal, State, and international government and private sector stakeholders, the NCSD CEP utilizes exercises as a forum to discuss current and potential threats as well as possible solutions in a non-attribution setting.

Exercises provide the opportunity to evaluate and validate existing plans, processes, and procedures. Throughout the development and execution of an exercise, various attack scenarios are explored and rehearsed in a controlled venue to address prevention and mitigation strategies;

evaluate plans, processes and procedures currently in place; and examine policy issues, ultimately intended to develop lessons learned and post-exercise action plans that will better secure the Nation's CIKR sectors.

Without proper information sharing relationships and communication paths, our Nation will not be adequately prepared to protect or defend itself during an attack on any of the CIKR sectors, cyber or otherwise. Exercises are an excellent environment where these relationships can be built and strengthened not only in the interagency arena but with the private sector as well.

AREA F.7: United States Computer Emergency Readiness Team (US-CERT)

Focus Area: Trusted Relationships, Analysis and Warning Capabilities, Information Sharing, FISMA Compliance, Policy and Guidance

Lead Agency: Department of Homeland Security (DHS), Office of Cybersecurity and Communications, National Cyber Security Division,

Description
US-CERT Operations leads a public-private partnership to protect and defend the Nation's cyber infrastructure. US-CERT serves as the national focal point for coordinating cyber security issues affecting the Nation's infrastructure to include analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities. US-CERT coordinates information sharing with Federal agencies, State and local governments, private sector partners, infrastructure owners and operators, international allies, and the public to collect and disseminate cyber security threat and attack information

Expected Outcomes
- Understanding and analysis of the malicious code and other attack tools and development of countermeasures or recommend courses of action to combat malicious code that targets or exploits the U.S. Federal government and/or critical infrastructure.
- Means to gather cyber information prior to attacks and use that information to prevent attacks, protect cyber infrastructure, and restore infrastructure when attacks are successful.
- Alerts and warnings to build public awareness of the shared responsibility to protect individual cyber and communications networks.
- Increased situational awareness for Federal agencies and the Nation's cyber infrastructure so that they reduce cyber threats and vulnerabilities through identification, analysis, and comprehension of broad network activity, cyber security trends, and incident handling

Accomplishments
- Created and published Quarterly Trends and Analysis Report for public constituents and streamlined the publishing process. (Q3FY06, Q4FY06, Q1-Q4FY07)
- Created a web site for the Homeland Secure Data Network to facilitate US-CERT dissemination of important and SECRET classified information with constituents in the Intelligence Community. (Q2FY07)
- Implemented a plan to redesign the public US-CERT web site so that it better features and highlights the National Cyber Security Alert System. (Q3FY07)
- Verified, updated, and confirmed the alert system's SOPs. (Q4FY07)
- Deployed Einstein at a total of 13 Federal agencies. (Q4FY07)
- Created a new mailing list notifying the public of Current Activity. (Q4FY07)
- Completed concept paper and budget requests for increased operational capacity. (Q4FY07)
- Drafted US-CERT Private Sector CONOPS. (Q4FY07)
- Provided on-site incident response to twelve agencies. (Q3-Q4FY07)
- Provided on-site incident response to forty agencies. (Q1-Q3 FY08)
- Redesign the public US-CERT web site to better feature and highlight the National Cyber Security Alert System. (Q2 FY08)
- Produce detailed reports of analysis activity for the purpose of informing and educating response personnel. (Q2 FY08)

- Installed upgraded incident handling (Remedy) software on the Mission Operating Environment. (Q2 FY08)

Milestones

Q2FY08

- Finalize Trusted Internet Connection (TIC) requirements and request, receive, and evaluate Department and Agency plans to reduce and consolidate connections

Q3FY08

- Release list of Departments and Agencies that will be Trusted Connection Access Providers

Q4FY08

- Continue to work with the National Institute of Standards and Technology(NIST) to expand the National Vulnerability Database, a US Government repository of standards based vulnerability management data.
- Deploy Einstein sensors at additional Federal agencies.
- Annually verify, update, and confirm the US-CERT Operation's SOPs.
- Continue to work with international partners, specifically the U5 group of nations.
- Partner with additional private entities to market live feed that attracts a new subscriber base.

Q1FY09

- Finalize EINSTEIN System Program Baseline Documentation
- EINSTEIN 2.0 Phase I Complete

Q2FY09

- Enhance and expand data storage center for Einstein.
- EINSTEIN 3.0 Concept Development and System Evaluation
- Produce detailed reports of analysis activity for the purpose of informing and educating response personnel.

Q3FY09

- EINSTEIN 2.0 Phase II Complete for first 30 sites (TBR on Agency schedule)
- EINSTEIN 2.1 System Definition (vizualation and collaboration)

Q4FY09

- Develop implementation plan for alternative operations center outside the region.
- Deploy Einstein sensors at additional Federal agencies.
- EINSTEIN 2.1 Operational IOC
- Annually verify, update, and confirm the US-CERT Operation's SOPs.
- Continue to work with international partners, specifically the U5 group of nations.
- Partner with additional private entities to market live feed that attracts a new subscriber base.
- Continue to work with NIST to expand the National Vulnerability Database, a US Government repository of standards based vulnerability management data.

FY10 – FY13

- Deploy Einstein sensors at additional Federal agencies.
- Annually verify, update, and confirm the US-CERT Operation's SOPs.
- Continue to work with international partners, specifically the U5 group of nations.

- Provide space for industry personnel to physically reside in US-CERT Operations Center.
- Continue to expand the National Vulnerability Database.
- Continue to produce detailed reports of analysis activity for the purpose of informing and educating response personnel.

Impediments/Challenges
As the demand for US-CERT capabilities grows, current Federal staff is at capacity with analysis, project management, and outreach responsibilities, and the program needs additional contracting support. In addition, increased demand for the production of alerts and bulletins and the desire for more frequent updates to the web site and portal require an increase in Federal full time equivalents (FTE) and contract support. While US-CERT is making progress against its staffing goals which has decreased the demand on existing staff, until US-CERT is able to achieve its staffing goals, the challenge will remain. Also, the process to sign memorandum of understanding between DHS and agencies poses slight delays in the growth of the Einstein program.

Metrics
NCSD is in the process of revising our program-level metrics for the referenced program to ensure they adequately address the specific focus areas and provide insight into program efficiency and results.

Remarks
US-CERT is the primary Federal agency charged with promoting and coordinating the cybersecurity of the Federal IT infrastructure to help secure and defend the nation from cyber events, incidents, intrusions and attacks. US-CERT's incident handling, analysis, situational awareness, and production programs help prepare for and deter against catastrophic cyber incidents by achieving a collaborative risk management and deterrence capability. The programs work together to promote public awareness and a coordinated, national response system for major cyber disruptions.

US-CERT coordinates with the NCC, other DHS entities, Federal departments and agencies, State and local governments through the Multi-State ISAC, the private sector through the NIPP Sector partnership framework, and international governments, including the UK, Canada, Australia, New Zealand, and others.

US-CERT disseminates timely and actionable cyber security information, alerts, and warnings to homeland security partners and the American public to improve cyber awareness and help protect critical information networks. Information is disseminated through several mechanisms, including but not limited to two web sites:

- The **public US-CERT web site** is an information source for citizens, private enterprise, IT professionals, and Federal agencies. The website features regularly updated summaries of cyber security incidents and issues, and it disseminates this information through "really simple syndication" feeds and subscriber mailing lists. The program's primary information product is the National Cyber Alert System, which includes Technical Cyber Security Alerts, Cyber Security Alerts, Cyber Security Bulletins, and Cyber Security Tips. Additional information products include Current Activity, Vulnerability Notes, the Vulnerability Knowledgebase, and Quarterly Trends and Analysis Reports.

- The **US-CERT Secure Portal** provides sensitive unclassified, cyber security information to ISACs, the Government Forum of Incident Response and Security Teams, and other key vetted stakeholders. The program posts information products for its secure portal constituents, including Situational Awareness Reports, Technical Information Papers, Federal Information Notices, Critical Infrastructure Information Notices, Quarterly Trends Reports, and other alerts.

US-CERT's situational awareness capability consists of the following initiatives:

- Mission Operating Environment (MOE) – A collection of hardware and software that provides an operating platform that is sequestered from the Internet, separate from the DHS Local Area Network, and supports the US-CERT's cyber security operations. The MOE provides US-CERT with the capability to conduct incident handling, analysis, and information sharing safely and securely without infecting computing infrastructure that supports DHS operations.

- Einstein – A collection of hardware and software that supports an automated process to collect, correlate, analyze, and share cyber security information across Federal government networks. Einstein collects data flows in real time from participating Federal agency Internet connections and provides an enhanced view and analysis of the health of critical cyber networks across the U.S. Government. The program provides a knowledge base for improving network security, resulting in increased resiliency of critical electronically delivered government services.