National Infrastructure Protection Plan

2007/2008 Update

Homeland
Security

Table of Contents

National Infrastructure Protection Plan 2007/2008 Update

Overview

The National Infrastructure Protection Plan (NIPP) sets forth a comprehensive risk management framework and clearly defines critical infrastructure protection roles and responsibilities for the Department of Homeland Security (DHS); Sector-Specific Agencies (SSAs); and other Federal, State, local, tribal, territorial, and private-sector security partners. The NIPP provides a coordinated approach for establishing national priorities, goals, and requirements for infrastructure protection so that funding and resources are applied in the most effective manner. The NIPP risk management framework responds to an evolving risk landscape; as such, there will always be changes to the NIPP—from relatively minor to more significant. The 2006 NIPP established the requirement to fully reissue the plan every three years to ensure that it is current and of maximum value to all security partners. However, it is also important to provide periodic reviews to identify and address significant issues so that all security partners have an awareness of these issues and their potential impact.

This NIPP Update is a stand-alone document that provides a brief overview of the most significant and relevant issues or changes to the NIPP since its release in June 2006. Because significant program changes were identified in late 2007 and realized in early 2008, a separate 2007 Update was not released. This document presents both 2007 and 2008 updates to the NIPP. Specifically, it addresses:

- Establishment of the 18th CIKR sector
- Sector name changes
- Education Facilities Subsector
- Evolution of National Asset Database to Infrastructure Data Warehouse
- NIPP Critical Infrastructure and Key Resources (CIKR) Protection Metrics
- Update on the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC)
- Regionalization of the NIPP Partnership Model
- Critical Foreign Dependencies Initiative
- Homeland Security Information Network (HSIN) update
- Further definition of the CIKR Information-Sharing Environment (ISE)
- Critical Infrastructure Warning Information Network (CWIN)
- Chemical security regulation released
- Sector-Specific Plans (SSPs) published
- Evolution from the National Response Plan to the National Response Framework
- NIPP Education, Training, Outreach and Awareness

- Research and Development Planning – Integrated Product Teams
- National Infrastructure Simulation and Analysis Center (NISAC)
- Cross-sector cybersecurity
- Protection and resiliency
- DHS organizational changes: National Protection and Programs Directorate (NPPD)

Several of the discussions provide points of contact or links to additional information.

This document is intended to meet the requirement for an annual review and update of the NIPP to maintain the NIPP's relevance as a national strategy for both public and private-sector security partners in protecting our Nation's CIKR. In parallel with the annual review process, comments were and will continue to be solicited for inclusion in the reissue of the NIPP in 2009. Both detailed and strategic comments are welcome. The content of this 2007/2008 Update document will be included in the triennial NIPP review/revision process, which is currently underway.

This update document tracks the organization of the NIPP, describing the updates and changes to each chapter in the NIPP, beginning with the Executive Summary. If there are no changes to a given chapter or appendix, this is noted as well. Several overarching issues that are not specific to any given chapter are addressed at the end of the document.

Executive Summary

Establishment of the 18th CIKR Sector – Critical Manufacturing

On March 3, 2008, DHS formally established the Critical Manufacturing Sector as the 18th CIKR sector, for which DHS' Office of Infrastructure Protection (IP) is designated as the SSA. Based on guidance contained in Homeland Security Presidential Directive 7, DHS concluded that nine elements within four manufacturing industries meet the Department's definition of a CIKR sector. These industries are not included in the 17 previously designated sectors.

Manufacturing Industry	Element
1. Primary Metal Manufacturing	▪ Iron and Steel Mills and Ferro Alloy Manufacturing
	▪ Alumina and Aluminum Production and Processing
	▪ Nonferrous Metal (except Aluminum) Production and Processing
2. Machinery Manufacturing	▪ Engine, Turbine, and Power Transmission Equipment Manufacturing
3. Electrical Equipment, Appliance, and Component Manufacturing	▪ Electrical Equipment Manufacturing
4. Transportation Equipment Manufacturing	▪ Motor Vehicle Manufacturing
	▪ Aerospace Product and Parts Manufacturing
	▪ Railroad Rolling Stock Manufacturing
	▪ Other Transportation Equipment Manufacturing

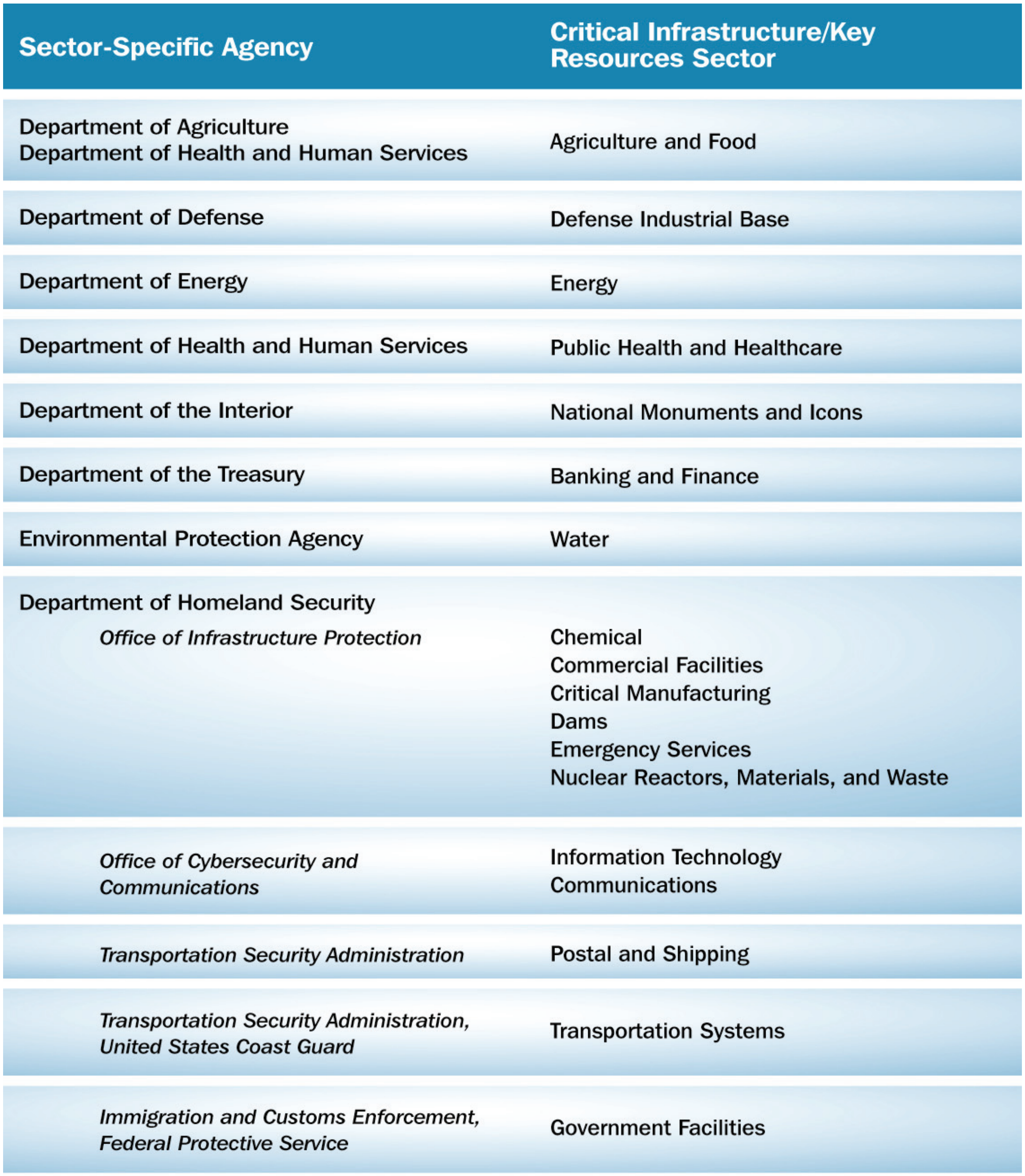
Sector Name Changes

To better reflect the scope of three sectors, DHS has recognized the following name changes:

Original Name	New Name
Commercial Nuclear Reactors, Materials and Waste	Nuclear Reactors, Materials and Waste
Drinking Water and Water Treatment Systems	Water
Telecommunications	Communications

Table S-1 is updated to reflect these sector name changes and the addition of the Critical Manufacturing Sector, as follows.

Table S-1. Sector-Specific Agencies and CIKR Sectors



Sector-Specific Agency	Critical Infrastructure/Key Resources Sector
Department of Agriculture Department of Health and Human Services	Agriculture and Food
Department of Defense	Defense Industrial Base
Department of Energy	Energy
Department of Health and Human Services	Public Health and Healthcare
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Water
Department of Homeland Security *Office of Infrastructure Protection*	Chemical Commercial Facilities Critical Manufacturing Dams Emergency Services Nuclear Reactors, Materials, and Waste
Office of Cybersecurity and Communications	Information Technology Communications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration, United States Coast Guard	Transportation Systems
Immigration and Customs Enforcement, Federal Protective Service	Government Facilities

Chapter 1. Introduction

There are no changes or updates to this chapter.

Chapter 2. Authorities, Roles, and Responsibilities

Establishment of the 18th CIKR Sector – Critical Manufacturing

Section 2.2.1 of the NIPP discusses the roles and responsibilities of DHS in CIKR protection. The second paragraph of this section is updated to note that DHS now serves as the SSA for 11 CIKR sectors and Critical Manufacturing is added to the list.

Table 2-1 is updated to include the Critical Manufacturing Sector. (This change is reflected in revised Table S-1 above.)

Education Facilities Subsector

In keeping with section 2.2.2 of the NIPP, DHS has recognized the Department of Education's Office of Safe and Drug-Free Schools (OSDFS) as the lead for Education Facilities (EF), a subsector of the Government Facilities Sector. In this role, EF coordinates with Federal and non-Federal security partners to help address risk management for the subsector. EF refers to pre-kindergarten and all K-12 through post-secondary public, private, and proprietary education facilities. As the SSA for EF, OSDFS helps to address CIKR protection efforts in the subsector and works closely with the DHS Federal Protective Service, which is the overall lead for the Government Facilities Sector. EF assets and systems vary dramatically—from pre-kindergarten to colleges and universities and from smaller schools housing fewer than a hundred students to large schools housing several thousand students. EF also includes campus grounds and dormitories, increasing the number of facilities and the level of complexity and challenge to risk mitigation.

All subsector CIKR protection efforts are designed to support EF's overall vision: "That all schools and universities are ready to prevent-mitigate, prepare for, respond to, and recover from all hazards, natural or man-made, by having a comprehensive, all-hazards plan based on the four phases or key principles of emergency management to enhance school safety, to minimize disruption, and to ensure continuity of the learning environment."

Chapter 3. The Protection Program Strategy: Managing Risk

Evolution of National Asset Database to Infrastructure Data Warehouse

As described in section 3.2.1 of the NIPP, successful protective programs require the collection, maintenance and protection of information on the assets, systems, networks, and functions that comprise the Nation's infrastructure. The Office of Infrastructure Protection's (IP) Infrastructure Information Collection Division (IICD) leads DHS' effort to protect and provide standardized and relevant infrastructure information to homeland security partners. Partial functions of the previously existing National Asset Database (NADB) have been combined with emergent capabilities to form a new, integrated system called the Infrastructure Data Warehouse (IDW). The IDW establishes a distributed information technology (IT) architecture that integrates data bases from Federal, State, and commercial sources by linking the existing data stores through a larger, virtual IT structure. IDW will improve data quality by allowing numerous partners and entities within the homeland security community to collect, maintain and verify their own data in the system. This architecture reduces duplication of effort and enhances the robustness of existing information. Technical and data standards used by the IDW architecture will be provided as needed to facilitate compatibility and interoperability of systems and enable efficient information sharing among security partners.

The IDW is one element of the Infrastructure Information Collection Program (IICP) – an innovative initiative that integrates independent systems, tools and capabilities to form an interoperable capability and workflow that supports and sustains information management and exchange. A key component of the IICP is the Constellation Automated Critical Asset Management System (C/ACAMS). C/ACAMS is a secure, Web-based information services portal that supports infrastructure protection efforts at the State and local level. It allows the user to manage the collection and effective use of asset data and provides access to a comprehensive set of tools and resources for developing and implementing protective programs. C/ACAMS is focused primarily on pre-incident prevention and protection efforts but also provides assistance for post-incident response.

NIPP CIKR Protection Metrics

As discussed in section 3.6 of the NIPP, metrics help to: (1) assess the progress made in achieving security goals and (2) drive continuous improvement of CIKR protection measures. The NIPP CIKR protection metrics process (Exhibit 1) includes four metrics areas, as described below. These activities are supportive of four principal objectives in achieving the NIPP goal:

- Understanding and sharing information about terrorist threats and other hazards;
- Building security partnerships to share information and implement CIKR protection programs;
- Implementing a long-term risk management program; and
- Maximizing efficient use of resources for CIKR protection.

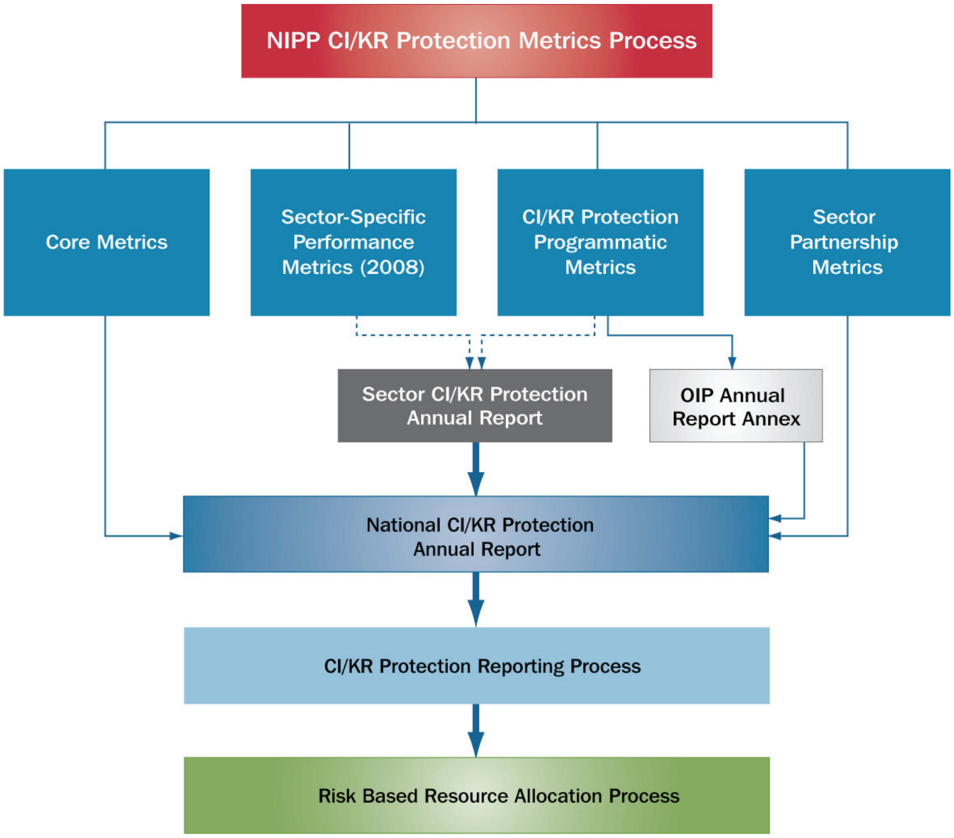

NIPP CI/KR Protection Metrics Process
Core Metrics
Sector-Specific Performance Metrics (2008)
CI/KR Protection Programmatic Metrics
Sector Partnership Metrics
Sector CI/KR Protection Annual Report
OIP Annual Report Annex
National CI/KR Protection Annual Report
CI/KR Protection Reporting Process
Risk Based Resource Allocation Process

Exhibit 1: NIPP CIKR Protection Metrics Process

1. Core metrics represent a common set of measures that are tracked across all sectors. They include descriptive, process, and outcome measures that help DHS assess progress in implementing the NIPP and the SSPs. Core metrics enable comparison and analysis among different types of CIKR sectors and assist with resource allocation decisions. The primary responsibility for developing and tracking core metrics lies with DHS/IP. Core metrics data are collected annually from the SSAs, most recently in 2007. The 2007 NIPP Core Metrics questions requested information on both the status and, to the extent possible, the progress of each of the 17 original CIKR sectors in implementing the activities articulated in the NIPP and the SSPs. The 2008 NIPP Core Metrics are currently under development and build on and refine the 2007 NIPP Core Metrics.

2. Sector-specific performance metrics are the set of measures tailored to the unique characteristics of each sector. These measures contribute to the NIPP goal by addressing the specific protection challenges that the sector faces and the distinct business and/or operational continuity needs for each sector. They reflect the sector-specific characteristics (e.g., ownership patterns, degree of interdependency, type and distribution of assets, regulatory requirements) that drive the sector's security needs. They also reflect metrics and benchmarks that the asset owners and operators and other security partners agree can help drive progress toward achieving sector security goals. The primary responsibility for developing and tracking sector-specific metrics lies with the SSAs. Data regarding sector-specific metrics will be collected on a timetable determined by each sector. Most sectors will not begin collecting sector-specific data, for purposes of the NIPP, until 2009.

3. CIKR protection programmatic metrics are used to measure the effectiveness of specific programs, initiatives, and investments that are managed by Government agencies and sector partners. These metrics help to identify which programmatic efforts are having the greatest impact (e.g., risk reduction, cost effectiveness) in improving CIKR protection. The primary responsibility for developing and tracking programmatic metrics within each sector lies with the SSAs. Programmatic metrics are currently under development; data will be collected on a timetable determined by each sector.

4. Sector partnership metrics are used to assess the status of activities conducted under the sector partnership. Currently, these are developed and tracked by IP for all sectors.

The core and sector-specific performance metrics together provide a basis for addressing the possible impact of CIKR protection as a whole (i.e., *what* results are being achieved). The partnership and programmatic metrics show – in quantitative terms – the means used to achieve CIKR protection, as well as restoration and recovery (i.e., *how* results are being achieved). Together, these four types of metrics provide an overall picture of the status and effectiveness of the national CIKR protection effort and help align programs and enable resource decisions on the basis of current and reliable information.

The NIPP calls for DHS and the SSAs to work together to assess and report on the progress made in achieving sector goals. The assessment and progress reporting are components of the *Sector CIKR Protection Annual Reports* required by Homeland Security Presidential Directive 7 for each sector. While DHS is responsible for measuring progress across all CIKR sectors, each SSA is responsible for measuring progress within its own sector or subsectors. Core and sector-specific metrics will be used for sector and subsector reporting. Programmatic metrics will be used for individual program reporting.

For their 2008 Annual Report, each SSA will be asked to report on the proposed process to be used by the sector to identify, collect, and improve sector-specific metrics. Reporting of sector-specific metrics will not be requested for the 2008 Sector Annual Reports. Metrics for successive years will build on the work that has been outlined in the SSPs and identified or discussed in the 2008 Sector Annual Reports. The 2009 Sector Annual Reports are the targets for a sector-wide metrics collection and reporting effort.

Chapter 4. Organizing and Partnering for CIKR Protection

Update on the State, Local, Tribal and Territorial Government Coordinating Council (SLTTGCC)

As discussed in section 4.1.2.2 of the NIPP, in order to bring together CIKR protection experts from the private sector and all levels of government, DHS enabled and facilitated formation of the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC). The SLTTGCC functions as a forum for State, local, tribal, and territorial government representatives to engage with the Federal Government and CIKR owners and operators within the Sector Partnership Model, to protect the Nation's critical infrastructure.

The SLTTGCC now has five working groups (see below) and also provides liaisons to all the sectors:

Policy and Planning Working Group

- Reviews DHS CIKR protection plans, such as the SSPs and the National Response Framework;
- Provides feedback from a State, local, tribal, and territorial (SLTT) perspective to DHS; and
- Is particularly well positioned to provide SLTT insight into Federal planning efforts and give a strong voice to the concerns of these levels of government.

Communication and Coordination Working Group

- Facilitates the release of coordinated SLTTGCC-related information to the SLTT community or other critical communities;
- Develops clearer and more direct channel of communication with and among SLTT CIKR leadership and SSAs, and with the Department on CIKR issues and plans; and
- Helps to identify and support platforms that enable members of the SLTT community to share best practices in the CIKR protection mission area.

Information-Sharing Working Group

- Helps the SLTTGCC to understand CIKR information sharing at the SLTT level, determine what practices are effective, and identify opportunities for integration with each other and Federal Government resources; and
- Constructs an analysis of the CIKR information-sharing landscape in the SLTT environment to appraise best practices and identify gaps, opportunities for leverage, or areas requiring enhancement.

Constellation/ACAMS Working Group

- Works to further develop the Constellation / Automated Critical Asset Management System tool and to promote enhanced efforts to protect critical infrastructure at all levels of government.

- Engages continually with the Infrastructure Information Collection Division (IICD) to upgrade the C/ACAMS systems and functions, improve system responsiveness, increase user friendliness, and improve on-the-ground inventorying processes.

Chemical-terrorism Vulnerability Information (CVI) Working Group

- Engages with the Infrastructure Security Compliance Division (ISCD) regarding the various elements of the Chemical Facilities Anti-Terrorism Standards (CFATS). Makes recommendations to ISCD on the promulgation of a CVI sharing process, in which state and local officials with a need to know can access data on risks of selected facilities that manufacture, store or otherwise use security-sensitive chemicals.

- Working with ISCD and the Office of General Counsel to finalize a reasonable and rationale approach to sharing CVI with the attendant measures to secure such information.

The SLTTGCC strives to achieve geographical diversity and broad discipline representation through its membership. Additional information may be obtained at http://www.dhs.gov/slttgcc

Regionalization of the NIPP Partnership Model

As discussed in section 4.1.3 of the NIPP, DHS coordinates with regional coalitions to enhance infrastructure protection efforts across geographical and jurisdictional boundaries. DHS is supporting efforts to broaden the NIPP partnership framework further to integrate and leverage the CIKR protection activities of States and localities and existing public and private sector partnerships. The Regional Coalition Initiative is a new DHS effort that will define a framework, through integration with the SLTTGCC, of regional CIKR entities that are actively engaged in infrastructure protection efforts with local agencies and multi-jurisdictional governmental organizations. The newly formed Regional Consortium Coordinating Council (RCCC) will provide further horizontal integration between the SCCs, GCCs, and CIKR owners and operators and will integrate the NIPP with the infrastructure protection initiatives and partnership mechanisms of existing regional coalitions.

Critical Foreign Dependencies Initiative

As discussed in section 4.1.4.1 of the NIPP, DHS coordinates with the U.S. Department of State (State) to work with international security partners to improve protection of CIKR critical to the U.S. DHS is currently collaborating with its infrastructure protection partners across the Federal Government to create a comprehensive inventory of infrastructure located outside the U.S. which, if disrupted or destroyed, would lead to loss of life in the U.S. or critically affect the Nation's economic, industrial, or defense capabilities.

The Critical Foreign Dependencies Initiative (CFDI) is a process designed to ensure that the resulting list of critical foreign dependencies is inclusive, representative, and leveraged in a coordinated and responsible manner. The Initiative involves three phases:

- Phase I – Identification: DHS, working with Federal infrastructure protection community partners, developed the first ever National Critical Foreign Dependencies List in FY2008, reflecting the critical foreign dependencies of the initial 17 critical infrastructure and key resource sectors, as well as critical foreign dependencies of interest to the Nation as a whole. The identification process will be conducted on a yearly basis, and include input from public and private sector infrastructure protection community partners.
- Phase II – Prioritization: DHS works with the Department of State and other infrastructure protection partners to prioritize the National Critical Foreign Dependencies List based on factors such as overall criticality of the element to the United States; risk to the element; and foreign partner willingness and capability to engage in risk management activities. The prioritization process will be conducted on a yearly basis.
- Phase III – Engagement: Phase III involves leveraging the prioritized National Critical Foreign Dependencies List to guide current and future U.S. bilateral and multilateral incident and risk management activities with foreign partners. DHS and State will establish mechanisms to ensure coordinated engagement in domestic coordination and collaboration by public sector entities.

Homeland Security Information Network (HSIN) Update

Section 4.2.3 and Appendix 3B (section 3B.3) of the NIPP pertain to HSIN, a homeland security-focused communications system developed by State and local authorities and connecting all 50 States, 5 territories, Washington, DC, and 50 major urban areas. HSIN is one of the key DHS technology tools for strengthening the protection and ensuring reliable performance of the nation's critical infrastructure through communication, coordination, and information sharing. It is an Internet-based platform that enables secure, encrypted sensitive but unclassified (SBU) and for official use only (FOUO) communication between DHS and vetted members within and across CIKR sectors.

HSIN Next Generation, or HSIN 3.0, will debut in the summer of 2008 and include new functionality for all users. HSIN 3.0 will improve upon the existing toolkit that HSIN-CS already offers and continue to strengthen the capability of all CIKR sectors to share sensitive information as well as improve coordination and communication between CIKR sectors and DHS.

Further Definition of the CIKR Information-Sharing Environment (ISE)

As follow-up to the original discussion of ISE in section 4.2.3 of the NIPP, the Program Manager (PM)-ISE formally issued the CIKR ISE paper in May 2007. The paper describes the core elements of robust information sharing with the CIKR sectors.

The PM-ISE adopted the CIKR ISE as the private sector component, with the Assistant Secretary for Infrastructure Protection as the designated Federal government lead. It is important to note that most of the information shared daily within the CIKR ISE consists of information necessary for coordination and management of risks resulting from natural hazards and accidents. For information sharing to be efficient and sustainable for the CIKR owners and operators, the same environment should be used to share terrorism information, albeit in a tailored manner.

CIKR information sharing breaks new ground. It also creates business risks for the owners and operators. Significant questions are raised, such as: What information is required for a productive two-way exchange? How is information most efficiently delivered and to whom to elicit effective action? How is information–both proprietary and government–appropriately protected? How will the sectors effect appropriate action in coordination with all levels of government? How can business risks be mitigated when an exchange takes place?

Of particular criticality is the coordination of CIKR information sharing at the national level with that at the local level, where most decisions are made and actions taken to support the CIKR protection mission. The integration of the CIKR ISE into the national ISE as its private sector component, in recognition of its comprehensiveness and engagement with all levels of government, strengthens the foundation for effective coordination.

The CIKR ISE supports three levels of decision making and action: 1) strategic planning and investment; 2) situational awareness and preparedness; and 3) operational planning and response. It provides for policy, governance, planning, and coordination of information sharing, as well as forums for developing effective, tailored forms and identifying the types of information necessary for security partners to make appropriate decisions and take necessary actions for effective risk management.

The CIKR ISE also encompasses a number of mechanisms that facilitate the flow of information, mitigate obstacles to voluntary information sharing by CIKR owners and operators, and provide feedback and continuous improvement for structures and processes. The CIKR ISE accommodates a broad range of sector cultures, operations, and risk management approaches and recognizes the unique policy and legal challenges for full two-way sharing of information between the CIKR owners and operators and various levels of government.

Critical Infrastructure Warning Information Network (CWIN)

An ISE addition since the 2006 release of the NIPP, CWIN is a mechanism that facilitates the flow of information, mitigates obstacles to voluntary information sharing by CIKR owners and operators, and provides feedback and continuous improvement for structures and processes. CWIN is the critical, survivable network connecting DHS with vital sector partners that are essential to restoring the Nation's core infrastructure. Those sectors/subsectors are Communications, IT, and Electricity, as well as their Federal and State official counterparts. In the circumstance where all or a major part of telecommunications and Internet connectivity are lost or disrupted, CWIN is designed to provide a survivable “out of band” communications and information-sharing capability to coordinate and support infrastructure restoration. Once the core capabilities of telecommunications, the Internet, and electricity are restored, normal communication channels can be utilized and other critical infrastructures can begin the process of restoration.

Release of Chemical Security Regulations

This information supplements section 4.3.2 of the NIPP, regarding chemical security. Section 550 of Public Law (P.L.) 109-295, entitled Making Appropriations for the Department of Homeland Security for the Fiscal Year Ending September 30, 2007, and for Other Purposes (October 4, 2006), authorizes DHS to use a Sensitive But Unclassified designation to protect information created and used to manage chemical facility anti-terrorism standards. Complying with this requirement, the *Chemical Facility Anti-Terrorism Standards Interim Final Rule* was issued on April 9, 2007.

Section 550 of the Homeland Security Appropriations Act of 2007 requires covered chemical facilities to prepare security vulnerability assessments and develop and implement Site Security Plans, which include measures that satisfy the risk-based performance standards established in the regulation (6 CFR Part 27). This information is protected under the regulation as Chemical-Terrorism Vulnerability Information. The rule details DHS processes for seeking compliance, including issuance of Orders Assessing Civil Penalty and Orders for the Cessation of Operations.

More information on the rule may be obtained at:
http://www.dhs.gov/xprevprot/laws/gc_1166796969417.shtm

Chapter 5. Integrating CIKR Protection as Part of the Homeland Security Mission

Sector-Specific Plans (SSPs) Published

As discussed in section 5.3.1 of the NIPP, the SSPs that support the NIPP were all submitted to DHS by December 31, 2006 and were officially released on May 21, 2007, after review and comment by the Homeland Security Council's Critical Infrastructure Protection Policy Coordinating Committee.

Those SSPs that are available for general release may be downloaded from: http://www.dhs.gov/nipp (click on Sector-Specific Plans). If an SSP is not posted there, it is marked as For Official Use Only (FOUO). For copies of the FOUO SSPs, please contact the responsible SSA, or the NIPP Program Management Office (NIPP@dhs.gov).

Evolution from the National Response Plan to the National Response Framework

This section updates the information in section 5.4.1 of the NIPP and speaks to the *National Response Framework*, which replaces the former *National Response Plan (NRP).* This framework represents a natural evolution of the national response architecture.

The *National Response Framework* establishes a comprehensive, national, all-hazards approach to domestic incident response. The framework presents an overview of key response principles, roles, and structures that guide the national response. It describes how communities, States, the Federal Government, and private-sector and nongovernmental partners apply these principles for a coordinated, effective national response. It also describes special circumstances where the Federal Government exercises a larger role, including incidents where Federal interests are involved and catastrophic incidents where a State would require significant support. Its real value, however, is in how these elements come together and are implemented by first responders, decision makers, and supporting entities to provide a unified national response.

The framework is written for senior elected and appointed leaders, such as Federal agency heads, State Governors, tribal leaders, mayors, or city managers – those who have a responsibility to provide for effective incident management. At the same time, it informs emergency management practitioners, explaining the operating structures and tools used routinely by first responders and emergency managers at all levels of government.

The Critical Infrastructure and Key Resources Support Annex (released in January 2008) is an important part of the National Response Framework in terms of CIKR protection. This annex describes policies, roles and responsibilities, and the concept of operations for assessing, prioritizing, protecting, and restoring CIKR of the United States and its territories and possessions during actual or potential domestic incidents. The annex details processes to ensure coordination and integration of CIKR-related activities among a wide array of public and private incident managers and CIKR security partners within immediate incident areas as well as at the regional and national levels.

Additional information can be found at http://www.fema.gov/emergency/nrf/

Chapter 6. Ensuring an Effective, Efficient Program Over the Long Term

NIPP Education, Training, Outreach and Awareness

As discussed in section 6.2 of the NIPP, training and education programs are essential to developing and maintaining the readiness of organizations and individuals and helping to ensure a consistent message and approach to CIKR protection among security partners. The NIPP establishes a framework to build national awareness and enable the education and training needed to ensure an effective, efficient CIKR protection program over the long term. National education and awareness efforts support NIPP-related programs, investments, and activities by ensuring a focused understanding of the all-hazards threat environment.

Education and Training

The goals of NIPP education and training programs include:

- Providing an integrated, coordinated approach that energizes and involves all security partners;
- Developing and implementing grassroots education programs that communicate effectively with key audiences; and
- Maximizing coordination, deepening relationships, and broadening participation and practices required to implement the NIPP and supporting SSPs.

DHS recently conducted a training needs assessment to gain a comprehensive understanding of the gaps and priority needs in NIPP training and education. The Sector-Specific Agencies were surveyed as part of the assessment, the results of which will be used to establish a national network of critical infrastructure training and education programs.

Academic and Research Programs

DHS works with a wide range of academic institutions to incorporate CIKR protection into professional education programs. For example, DHS collaborates with universities to incorporate homeland security-related courses into their curriculum and sponsors a degree program in homeland defense and security at the Naval Postgraduate School. In addition, DHS' Science and Technology Directorate (S&T) works with academic institutions to establish Centers of Excellence – university-based partnerships or federally funded research and development centers – to provide independent analysis of CIKR protection issues and offer higher education programs related to infrastructure protection.

DHS is promoting the development of a CIKR higher education program that will include CIKR academic degrees and adult education. The program is being developed through a collaborative effort across DHS, involving IP, the S&T Universities and Centers of Excellence Program, the Transportation Security Administration, and others. The initial program is being developed through the recently established National Transportation Security Center of Excellence (NTSCOE), which brings together a number of academic institutions with a mandate to build education and training programs relevant to the CIKR protection mission. This initiative provides a framework for the identification, development, and delivery of critical infrastructure courses in the transportation industry that include continuing education and employee training as well as college-level academic courses. While the initial focus is tailored to the Transportation Systems Sector, this initiative will lead to a multidisciplinary core curriculum applicable across all CIKR sectors.

Through a grant with the Department of Commerce's National Institute of Standards and Technology, the Critical Infrastructure Protection (CIP) Program at George Mason University funds basic and applied research and supports outreach activities related to CIP. Key areas of research have been cybersecurity, physical security, information sharing between the public and private sector, regional, State & local issues, and privacy concerns. The CIP Program also publishes *The CIP Report*, a monthly, electronic newsletter for professionals in industry, government, and academia with an interest in infrastructure protection.

The CIP Program supports DHS/IP in researching issues related to NIPP metrics and performance assessment. This research includes topics such as information collection, sharing, and use, as well as applicable authorities, and risk management training. The objective of this research is improved information sharing between the public and private sectors for the enhancement of infrastructure protection and the public-private partnership.

Outreach and Awareness Efforts

DHS defines two major goals for NIPP outreach and awareness:

Increase awareness of the NIPP and promote understanding of its importance to all security partners. To achieve this goal, DHS employs a multi-media approach to reach a broad and diverse audience. DHS has developed an interactive, online training course and video and is currently updating a series of one-page printed snapshots discussing each CIKR sector and other NIPP-related topics. The NIPP trade show booth and printed collateral materials are available for DHS and sector use at conferences and other events. In addition, DHS coordinates with the sectors to produce sector-specific outreach and awareness materials, such as the Security Awareness Guide and Protective Measures Handbook developed by the Dams Sector.

Foster a NIPP community of practice with shared learning. DHS is creating and expanding automated tools to support information sharing among security partners, including enhancements to the NIPP pages on the DHS website and the launch of a NIPP Channel on DHS' Lessons Learned Information Sharing (LLIS) website. The NIPP Newsletter provides monthly updates on DHS and sector programs and initiatives in CIKR protection. In 2008, the NIPP Newsletter was converted to HTML format, making it more interactive and user-friendly to an ever-growing distribution of NIPP security partners.

Recently, DHS developed a National CIKR Protection Outreach and Awareness Strategy, the goal of which is to motivate the public and private sectors to take and support actions to protect America's CIKR using the framework identified in the NIPP. As part of this effort, DHS is providing guidance to the CIKR sectors in developing their own sector-specific strategies for outreach and awareness. In addition, DHS is working closely with the sectors to develop “NIPP In Action” stories that provide real-world examples of NIPP implementation. These stories are available in multi-media format for use in a variety of settings, including one-page snapshots, poster boards, and video clips.

Research and Development Planning - Integrated Product Teams

As described in section 6.3.3 of the NIPP, DHS developed a Research and Development (R&D) plan to guide national R&D activities in critical infrastructure protection. As part of this effort, DHS instituted Integrated Product Teams (IPTs) to enhance support for R&D planning and program oversight. DHS works with the sectors through the IPT process, to identify and address R&D requirements and capability gaps. IPTs serve not only as a forum for potential users of R&D; they also include those who sponsor and execute R&D projects to ensure that these programs match CIKR protection needs. IPTs are managed jointly by DHS’ Science and Technology Directorate (S&T) and its DHS “customer” organizations, such as the Office of Infrastructure Protection. IPTs govern those R&D programs that will potentially transition to operational use within a few years.

National Infrastructure Simulation and Analysis Center (NISAC)

As discussed in section 6.4.2 of the NIPP, the NISAC is a modeling, simulation, and analysis (MS&A) program composed of roughly 100 personnel from Sandia National Laboratories and Los Alamos National Laboratory. NISAC is mandated by Congress to be a “source of national expertise to address critical infrastructure and key resources (CIKR) protection” research and analysis. NISAC prepares and shares analyses of CIKR, including their interdependencies, vulnerabilities, consequences, and other complexities; under the direction of IP.

While the 2001 PATRIOT (Provide Appropriate Tools Required to Intercept and Obstruct Terrorism) Act established the requirement for NISAC, the Homeland Security Appropriations Act of 2007 specifies its current mission. NISAC is required to provide “modeling, simulation, and analysis of the assets and systems comprising CIKR in order to enhance preparedness, protection, response, recovery, and mitigation activities.” The Center is also directed to share information with Federal agencies and departments that have CIKR responsibilities.

NISAC’s objectives cover two main areas of focus:

- Provide operational support to DHS and other Federal Government entities on an as-needed basis in the form of analysis, simulation, and scenario development; and
- Develop long-term capabilities by maintaining expertise in the application of analysis tools and the development of improved processes and tools in support of longer-term DHS projects.

NISAC accomplishes its mission through three types of products:

- Pre-planned long-term analyses;
- Pre-planned short-term analyses; and

Unplanned priority analytical projects that are based on higher-level tasking or that are related to real-time threats to critical infrastructure (e.g., hurricanes).

NISAC accesses CIKR information and data from a variety of government CIKR sectors and a wide range of private sector sources, including other participants in CIKR protection projects and programs. NISAC uses some data that are considered proprietary to a single industry – or even to a specific firm; these data must, therefore, be protected from unrestricted dissemination in order to maintain the trust of the information providers. However, NISAC products principally serve government decision makers, who can derive valuable insight into incident consequences at a higher level than the supporting data could provide.

Chapter 7. Providing Resources for the CIKR Protection Program

There are no changes or updates to this chapter.

List of Acronyms and Abbreviations

The following acronyms are updated to reflect a policy change in the way the acronyms are written.

CIKR	Critical Infrastructure and Key Resources
IP	Office of Infrastructure Protection (within DHS' National Protection and Programs Directorate)

The following acronym is updated to reflect the inclusion of territorial governments on the coordinating council.

SLTTGCC	State, Local, Tribal, and Territorial Government Coordinating Council

The following acronyms are added to the list.

CFATS	Chemical Facility Anti-Terrorism Standards
RCCC	Regional Consortium Coordinating Council

Glossary of Key Terms

The following definition is added to the Glossary, between the definitions of *Business Continuity* and *Consequence*.

Chemical Facility Anti-Terrorism Standards. On April 9, 2007, DHS issued the Chemical Facility Anti-Terrorism Standards (CFATS). Congress authorized this interim final rule (IFR) under Section 550 of the Department of Homeland Security Appropriations Act of 2007, directing the Department to identify, assess, and ensure effective security at high-risk chemical facilities.

The definition of *Sector* is updated to reflect the establishment of an 18th CIKR sector, as follows:

Sector. A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society. The NIPP addresses 18 CIKR sectors, as identified by the criteria set forth in HSPD-7.

Appendix 1: Special Considerations

Appendix 1A: Cross-Sector Cybersecurity

General discussions addressing cyber issues are found throughout the NIPP and in Appendix 1A. The National Cybersecurity Division (NCSD) is working closely with the SSAs and other security partners to integrate cybersecurity into the CIKR sectors' protection and preparedness efforts. These efforts will necessitate close scrutiny by each SSA of their own SSP to ensure there is a focus on identifying critical cyber infrastructure, assessing cyber risk and promoting voluntary assessments, implementing protective programs, and measuring the effectiveness of their efforts. NCSD actively collaborates with the individual sectors on cyber elements that should be considered for inclusion in the respective SSPs and Sector CIKR Protection Annual Reports. In addition, NCSD continues to work with sectors to reduce cyber risk and enhance cybersecurity.

There are no changes or updates to Appendix 1B.

Appendix 2: Authorities, Roles, and Responsibilities

There are no changes or updates to Appendices 2A and 2B.

Appendix 3: Managing Risks

There are no changes or updates to Appendices 3A, 3B and 3C.

Appendix 4: Organizing and Partnering for CIKR Protection: Existing Coordination Mechanisms

There are no changes or updates to Appendix 4.

Appendix 5: Integrating CIKR Protection as Part of the Homeland Security Mission

There are no changes or updates to Appendices 5A and 5B.

Appendix 6: Research and Development to Improve CIKR Protection Capabilities

There are no changes or updates to Appendix 6.

Overarching Issues

Protection and Resiliency

Questions have been raised about the focus of the NIPP on protection rather than resiliency. The NIPP defines protection as actions to mitigate the overall risk to CIKR assets, systems, networks, or their interconnecting links resulting from exposure, injury, destruction, incapacitation, or exploitation. In the context of the NIPP, protection includes actions to deter the threat, mitigate vulnerabilities, or minimize consequences associated with a terrorist attack or other incident. Protection includes a wide range of activities, such as hardening facilities, building resiliency and redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing security systems, promoting workforce surety, and implementing cybersecurity measures, among various others. Thus, protection should be interpreted as an overarching risk management strategy that fully acknowledges and supports the concept of resiliency where it offers the best solution to managing a particular risk or set of risks.

The NIPP explicitly recognizes that achieving the NIPP goal of building a safer, more secure, and more resilient America requires actions that address the following principal objectives:

- Understanding and sharing information about terrorist threats and other hazards.
- Building and sustaining security partnerships to share information and implement CIKR protection programs.
- Implementing a long-term risk management program that includes:
  - Hardening and ensuring the resiliency of CIKR against known threats and hazards, as well as other potential contingencies;
  - Processes to interdict human threats to prevent potential attacks;
  - Planning for rapid response to CIKR disruptions to limit the impacts on public health and safety, the economy, and government functions; and
  - Planning for rapid CIKR restoration and recovery for those events that are not preventable.
- Maximizing efficient use of resources for CIKR protection.

DHS Organizational Changes: National Protection and Programs Directorate (NPPD)

This section summarizes organizational changes within DHS related to roles and responsibilities described throughout the NIPP. NPPD (formerly the Preparedness Directorate) was formed in 2007 to advance the Department's risk-reduction mission. Reducing risk requires an integrated approach that encompasses both physical and virtual threats and their associated human elements. The components of NPPD include:

- **Office of Cybersecurity and Communications (CS&C)** has the mission to assure the security, resiliency, and reliability of the Nation's cyber and communications infrastructure in collaboration with the public and private sectors, including international partners. Specifically, CS&C is focused on preparing for and responding to catastrophic incidents that could degrade or overwhelm the networks, systems, and assets that operate our Nation's information technology (IT) and communications infrastructure. CS&C includes three divisions: the National Communications System, the National Cybersecurity Division, and the Office of Emergency Communications.
- **Office of Intergovernmental Programs (IGP)** has the mission to promote an integrated national approach to homeland security by ensuring, coordinating, and advancing Federal interaction with State, local, tribal, and territorial governments. The purpose of the office's operations is multi-faceted: To facilitate communication between the Department's expert resources and the expert resources of the Nation's autonomous governments; to act as an advocate for State, local, tribal, and territorial governments within the Department; and to coordinate and maintain constant awareness of the various bilateral communications occurring regularly throughout the Department. IGP's overarching goal is to facilitate timely and meaningful consultation by DHS and its agencies with our State, local, tribal, and territorial partners.
- **Office of Risk Management and Analysis (RMA)** will lead the Department's efforts to establish a common framework to address the overall management and analysis of homeland security risk. The office will serve as the DHS Executive Agent for national-level risk management analysis standards and metrics. It will develop and embed a consistent, standardized approach to risk. It will also develop a coordinated and collaborative approach to risk management that will allow the department to leverage and integrate risk expertise across components and external stakeholders. RMA will also assess DHS-level risk performance to ensure programs are measurably reducing risk across the country and communicate the DHS "risk story" in a manner that reinforces the value of the risk-based approach.
- **United States Visitor and Immigrant Status Indicator Technology (US-VISIT)** is part of a continuum of biometrically-enhanced security measures that begins outside U.S. borders and continues through a visitor's arrival in and departure from the United States.
- **Office of Infrastructure Protection (IP)** leads the coordinated national effort to reduce risk to our CIKR posed by acts of terrorism. In doing so, DHS increases the Nations' level of preparedness and the ability to respond and quickly recover

> in the event of an attack, natural disaster, or other emergency. IP facilitates the identification, prioritization, coordination, and protection of CIKR in support of Federal, State, local, tribal and territorial governments, as well as the private sector and international entities. By ensuring the sharing of information with our security partners, IP communicates threats, vulnerabilities, incidents, potential protective measures, and best practices that enhance protection, response, mitigation, and restoration activities across the Nation and the international community.

IP also realigned its organization in 2007 to (1) increase the efficiency and effectiveness of its programmatic activities, (2) reduce duplicative efforts, and (3) account for its new regulatory authority over chemical security compliance (P.L. 109-295, the Homeland Security Appropriations Act of 2007). The new organizational structure consolidates similar programs into and fosters functional integration and coordination among six divisions:

- **Infrastructure Security Compliance Division (ISCD)** leads the implementation of the Chemical Facility Anti-Terrorism Standards, balancing regulatory authority and the need to secure the Nation's highest risk chemical facilities with the sustained economic vitality of the Chemical Sector. ISCD develops and implements a program that aggressively assesses high-risk chemical facilities, promotes collaborative security planning, and ensures that covered facilities meet risk-based performance standards.
- **Infrastructure Information Collection Division (IICD)** leads the Department's efforts to acquire and provide standardized, relevant, and customer-focused infrastructure information to various public and private sector homeland security partners.
- **Infrastructure Analysis and Strategy Division (IASD)** leads the Nation's premiere analytical teams in the conduct of modeling, simulation, and analysis for IP in support of DHS and NIPP partners.
- **Protective Security Coordination Division (PSCD)** reduces the risk to the Nation's CIKR from a terrorist attack by (1) assessing vulnerabilities and consequences; (2) developing, implementing, and providing national coordination for protective programs; (3) facilitating response and recovery operations in an all-hazards environment; and (4) coordinating national and intergovernmental bombing prevention efforts; conducting requirements, capabilities, and gap analyses; and promoting information sharing and bombing prevention awareness.
- **Contingency Planning and Incident Management Division (CPIMD)** coordinates and implements IP's CIKR preparedness activities in the areas of exercises, contingency planning, concepts of operations development, and incident management in a manner that is consistent with and supportive of the NIPP and the National Response Framework, as well as establishes Department and Federal interagency incident management coordination structures.
- **Partnership and Outreach Division (POD)** develops and sustains viable strategic relationships and information-sharing systems and processes with the owners and operators of the Nation's CIKR that support program execution across the spectrum of preparedness, prevention, protection, response, and

recovery programs, which are reflected in the NIPP and its supporting SSPs, as they are implemented and monitored and their progress measured as reported in the National Annual Report.

Homeland
Security