2009 National Infrastructure Protection Plan
Frequently Asked Questions

The National Infrastructure Protection Plan (NIPP) provides the unifying structure for the integration of a wide range of efforts for the enhanced protection and resiliency of the Nation's critical infrastructure and key resources (CIKR) into a single national program. The Plan sets forth a comprehensive risk management framework and clearly defines related roles and responsibilities for the Department of Homeland Security (DHS), Federal Sector-Specific Agencies (SSAs), and other Federal, State, local, tribal, territorial, and private sector partners. The NIPP provides the coordinated approach used to establish national priorities, goals, and requirements for infrastructure protection and resiliency so that funding and resources are applied in the most effective manner.

The goal of the NIPP is to:

> *Build a safer, more secure, and more resilient America by preventing, deterring, neutralizing, or mitigating the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit elements of our Nation's CIKR and to strengthen national preparedness, timely response, and rapid recovery of CIKR in the event of an attack, natural disaster, or other emergency.*

Questions about the NIPP can be emailed to NIPP@dhs.gov. Alternatively, you can visit the NIPP web site at www.dhs.gov/nipp.

National Infrastructure Protection Plan Effective Date

Q: When was the NIPP released?
A: DHS originally issued the NIPP in June 2006 and just reissued it in January 2009. It will continue to evolve both in response to changing CIKR protection and resiliency needs and to incorporate increasingly refined processes, methodologies, and practices.

Critical Infrastructure and Key Resources Definition

Q: What are "critical infrastructure and key resources?"
A: CIKR includes systems and assets, whether physical or virtual, so vital to the United States that the incapacitation or destruction of such systems and assets would have a debilitating impact on national security, national economic security, public health or safety, or any combination of those matters.

Definitions of Protection and Resilience

Q: How does DHS define "protection?"
A: Protecting the Nation's CIKR is essential to making America safer, more secure, and more resilient in the context of terrorist attacks and other natural and manmade hazards. Protection includes actions to mitigate the overall risk to CIKR assets, systems, networks, functions, or their interconnecting links resulting from exposure, injury, destruction, incapacitation, or exploitation. In the context of the NIPP, this includes actions to deter the threat, mitigate vulnerabilities, or minimize the consequences associated with a terrorist attack or other manmade or natural disaster. Protection can include a wide range of activities such as improving security protocols, hardening facilities, building resiliency

and redundancy into systems, incorporating hazard resistance into facility design, initiating active or passive countermeasures, installing security systems, leveraging "self-healing" technologies, promoting workforce surety and screening programs, implementing cybersecurity measures, conducting training and exercises, and business continuity planning, among others.

Q: How does DHS define "resilience?"
A: The ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions.

Scope

Q: Is the NIPP about all hazards or just terrorist threats?
A: In accordance with the policy direction established in Homeland Security Presidential Directive 7 (HSPD-7), the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, and the National Strategy to Secure Cyberspace, the NIPP includes a special focus on the unique and potentially catastrophic impact of terrorist attacks. As part of the maturation process since the release of HSPD-7 in 2003, the NIPP now builds on and is structured to be consistent with and supportive of the Nation's all-hazards approach to homeland security preparedness and domestic incident management. Many of the benefits of enhanced CIKR protection are most sustainable when protective programs and resiliency strategies are designed to address all hazards.

CIKR Partners

Q: Who are the CIKR partners?
A: CIKR partners, or partners, are those Federal, State, regional, local, tribal, or territorial government entities; CIKR owners and operators and representative organizations; academic and professional entities; and not-for-profit and private volunteer organizations that share in the responsibility for protecting the Nation's CIKR.

Information-Sharing Environment

Q: What is the "information-sharing environment?"
A: To enable the protection of CIKR, DHS established an information-sharing network that is guided primarily by the NIPP and works in coordination with the efforts of the Federal Information-Sharing Environment (ISE). The ISE is concerned with improving the overall effectiveness of information sharing between and among Federal, State, and local government and the private sector. It is an element of the Intelligence Reform and Terrorism Prevention Act of 2004.

The CIKR ISE, developed under the NIPP, is the private sector component of the Federal ISE and is being implemented through the systematic development of information-sharing policies and the coordinated public-private sector implementation of core and enhanced mission-related information-sharing processes. For each level of decisionmaking and action, the CIKR ISE fosters the development of policy and governance processes to ensure coordination and clarity of roles and responsibilities.

Sector List

Q: What are the CIKR sectors?

A: The initial sectors set out in HSPD-7 are: Agriculture and Food; Banking and Finance; Chemical; Commercial Facilities; Communications; Dams; Defense Industrial Base; Emergency Services; Energy; Government Facilities; Healthcare and Public Health; Information Technology; National Monuments and Icons; Nuclear Reactors, Materials, and Waste; Postal and Shipping; Transportation Systems; and Water. In March 2008, the Secretary of Homeland Security added Critical Manufacturing as the 18th sector. HSPD-7 formally recognizes Maritime as a distinct sub-sector of the Transportation Systems Sector. Additionally, to address the unique requirements of Education Facilities, DHS recognizes it as a distinct sub-sector of the Government Facilities Sector.

Sector Points of Contact

Q: Who are the points of contact for each sector?

A: The President assigned responsibility for sector coordination to specific Federal departments and agencies known as Sector-Specific Agencies (SSAs). DHS is the SSA for the Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Emergency Services; Government Facilities; Information Technology; Nuclear Reactors, Materials, and Waste; Postal and Shipping; and Transportation Systems Sectors. Responsibility for coordinating efforts within the remaining sectors belongs to the Department of Agriculture (Agriculture and Food Sector); the Department of Health and Human Services (Healthcare and Public Health Sector and Agriculture and Food Sector); the Environmental Protection Agency (Water Sector); the Department of Energy (Energy Sector); the Department of Treasury (Banking and Finance Sector); the Department of Interior (National Monuments and Icons Sector); and the Department of Defense (Defense Industrial Base Sector).

Sector-Specific Plans

Q: What are Sector-Specific Plans?

A: Sector-Specific Plans (SSPs) complement the NIPP Base Plan and detail the application of the NIPP risk management framework specific to each of the CIKR sectors designated by HSPD-7. The SSAs completed the SSPs in coordination with their sector partners and submitted them in December 2006. The plans were released in May 2007. Distribution of SSPs is consistent with the appropriate level of classification. Some are marked *For Official Use Only* and must be handled accordingly. The SSPs are being rewritten in 2009 for release in 2010.

NIPP Implementation

Q: How is DHS implementing the NIPP?

A: DHS coordinates with CIKR partners through the sector partnership model to implement the NIPP risk management framework. This framework establishes the processes for combining consequence, vulnerability, and threat information to produce assessments of national or sector risk. The risk management framework is structured to promote continuous improvement to enhance CIKR protection by focusing activities on efforts to: set goals and objectives; identify assets, systems, and networks; assess risk based on consequences, vulnerabilities, and threats; establish priorities based on risk

assessments and, increasingly, on return-on-investment for mitigating risk; implement protective programs and resiliency strategies; and measure effectiveness. The results of these processes drive CIKR risk-reduction and management activities. DHS, the SSAs, and other CIKR partners share responsibilities for implementing the risk management framework.

Q: Who measures DHS's progress in implementing the NIPP and how?
A: DHS's Office of Infrastructure Protection is responsible for overseeing the implementation of the NIPP as well as leading its annual review. SSAs, in coordination with their Government and Sector Coordinating Councils, are responsible for establishing and maintaining the processes and practices needed for critical infrastructure protection in their sectors as well as the implementation of their SSPs. DHS reviews the progress of the sectors against the milestones set out in their SSPs.

In order to measure the effectiveness of the NIPP and SSPs, DHS uses metrics at the national and sector levels to measure progress and assess the effectiveness of the national and sector CIKR programs toward improving protection and resiliency and managing risk. The results of the metrics assessments feed into the annual reports to the President and Congress and into the OMB resource allocation process.

NIPP and SSP Revision Schedule

Q: How often are the NIPP and the SSPs revised?
A: The NIPP and SSPs include a process for annual review, periodic updates as required, and regularly scheduled full reviews and re-issuance every three years, or more frequently if directed by the Secretary of Homeland Security. The NIPP and SSP revision processes include development and updating of all documents based on lessons learned from CIKR protection and resiliency activities and changes in the national risk landscape.

Q: What information changed in the 2009 NIPP?
A: The 2009 NIPP captures the evolution and maturation of the processes and programs first outlined in 2006; it does not change policy. The revised NIPP integrates the concepts of resiliency and protection, and broadens the focus of NIPP-related programs and activities to an all-hazards environment. Some of the significant advances include:

- The issuance of the SSPs, which followed the release of the NIPP;
- Establishment of Critical Manufacturing as the 18th CIKR sector and the designation of Education as a subsector of Government Facilities;
- Expansion of the sector partnership model to include the geographically focused Regional Consortium Coordinating Council;
- CIKR mission integration within State and local fusion centers;
- Inclusion of outcome-focused performance measurement and reporting processes;
- Release of the Chemical Facility Anti-Terrorism Standards, establishing a regulatory framework for those industries that involve the production, use, and storage of high-risk chemicals; and
- Discussion of expanded CIKR protection-related education, training, outreach, and exercise programs.

Sector Partnership Model

Q: What is the Sector Partnership Model?
A: The NIPP relies on the sector partnership model as the primary organizational structure for coordinating CIKR efforts and activities. The sector partnership model encourages formation of Sector Coordinating Councils and Government Coordinating Councils, as well as cross-sector coordinating councils. These Sector and Government Coordinating Councils create a structure through which representative groups from Federal, State, local, tribal, and territorial governments and the private sector can collaborate and develop consensus approaches to CIKR protection. DHS provides guidance, tools, and support to enable these groups to work together to carry out their respective roles and responsibilities. Sector Coordinating Councils and corresponding Government Coordinating Councils work in tandem to create a coordinated national framework for CIKR protection within and across sectors.

State, Local, Tribal, and Territorial Coordination

Q: What is the cross-sector coordination mechanism for State, local, tribal, and territorial governments?
A: The State, Local, Tribal, and Territorial Government Coordinating Council provides an organizational structure to coordinate across jurisdictions on State- and local-level CIKR protection guidance, strategies, and programs. Composed of State, local, tribal, and territorial officials who are recognized leaders in CIKR protection and homeland security, the State, Local, Tribal, and Territorial Government Coordinating Council serves as a forum to ensure that they are fully integrated as active participants in national CIKR protection efforts. For more information, visit www.dhs.gov/slttgcc.

Regional Coordination

Q: How are regional impacts and interests addressed within the NIPP framework?
A: Because of the multitude of public and private sector partners involved, specific regional initiatives have a broad-reaching scope. In some cases, initiatives can even cross national borders and become international efforts. To better support these initiatives and further implement the NIPP, DHS supported the formation of the Regional Consortium Coordinating Council in July 2008. The mission of this council is to support and strengthen regional coalitions that enhance protection, response, recovery, and resilience of the Nation's CIKR.

Private Sector Collaboration

Q: Was the private sector involved in the development of the NIPP Base Plan?
A: Yes. Private sector input was an integral component of the NIPP development process for both the 2006 and 2009 versions of the NIPP. DHS and the SSAs worked closely with the CIKR Cross-Sector Council to engage the private sector and other owners and operators. Additionally, DHS went through two rounds of public comment as part of preparing each version of the NIPP.

Q: Have the SSPs been shared with the private sector?
A: Yes. Not only are the SSPs shared with private sector partners, they were developed in collaboration with the members of the Sector Coordinating Councils and other private

sector partners. The private sector is also an integral partner in the implementation of the SSPs. The sectors are engaging their owners and operators in the preparation and review of the 2010 SSPs.

International Participation in CIKR Protection

Q: Why does DHS involve itself in CIKR protection matters outside the United States?
A: Many U.S. CIKR assets, systems, and networks are interconnected with a global infrastructure that has evolved to support modern economies. Each of the CIKR sectors is linked in varying degrees to global energy, transportation, communications, information technology, and other infrastructure systems. This global system creates benefits and efficiencies, but also brings interdependencies, vulnerabilities, and challenges in the context of CIKR protection and resiliency.

Incentives for Private Sector Involvement

Q: What incentive does the private sector have to participate in NIPP-related activities?
A: Government can encourage industry to go beyond efforts already justified by their corporate business needs to assist in broad-scale CIKR protection by:

- Providing owners and operators timely, analytical, accurate, and useful information on threats to CIKR;
- Creating an environment that encourages and supports incentives for companies to voluntarily adopt widely accepted, sound security practices;
- Working with industry to develop and clearly prioritize key missions and enable their protection and/or restoration;
- Providing support for research needed to enhance future CIKR protection efforts; and
- Developing the resources to engage in cross-sector interdependency studies, through exercises, symposia, training sessions, and computer modeling that result in guided decision support for business continuity planning.

CIKR Protection Annual Reports

Q: How does DHS track progress on NIPP implementation at the sector and national level?
A: HSPD-7 requires SSAs to provide the Secretary of Homeland Security with annual reports on their efforts to identify, prioritize, and coordinate the protection of CIKR in their respective sectors. DHS works with SSAs to assess progress made toward goals in each sector based on these Sector CIKR Protection Annual Reports (Sector Annual Reports). DHS compiles the Sector Annual Reports into a cross-sector National CIKR Protection Annual Report that describes overall national progress toward CIKR protection. (Note: the National Annual Report is classified)

Protection of CIKR Information

Q: How is sensitive CIKR information protected?
A: The Protected Critical Infrastructure Information (PCII) Program was established pursuant to the Critical Infrastructure Information (CII) Act of 2002. The program institutes a means for the voluntary sharing of private sector and State and local CIKR

information with the Federal Government while providing assurances that the information will be exempt from public disclosure and will be properly safeguarded.

The PCII Program operates under the authority of the CII Act and the implementing regulation (6 Code of Federal Regulations Part 29) and defines both the requirements for submitting CII and those that governmental entities must meet for accessing and safeguarding PCII. For more information, contact pcii-info@dhs.gov. Additional PCII Program information may be found at www.dhs.gov/pcii.

Asset Identification

Q: Does the NIPP identify the specific CIKR assets for each sector?
A: No. The NIPP, through the risk management framework, establishes the processes for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national and sector risk. The sector utilizes this framework to identify specific critical infrastructure assets, systems, and networks that are unique to that sector. The NIPP does not contain information about specific assets, systems, or networks. The SSPs describe the types of assets, systems, and networks in each sector, but the plans do not contain actual inventories or discussions of specific assets or facilities.

Sector Risk Assessment Approach

Q: Are all sectors required to use the same approach for risk assessments?
A: No. The NIPP establishes core criteria for risk assessment methodologies. The criteria provide a guide for improving existing methodologies or modifying them so the investment and expertise they represent can be used to support national-level, comparative risk assessments and resource prioritization. DHS is sponsoring the development of various methodologies and tools to address the core criteria for risk assessment and national cross-sector risk assessment. Sectors are not required to use any specific methodology as long as they implement a methodology that meets the NIPP core criteria for risk assessment.

Q: How does DHS analyze threat and risk?
A: The DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) conducts integrated threat and risk analyses for CIKR sectors. HITRAC brings together intelligence and infrastructure specialists to ensure a sufficient understanding of the risks to the Nation's CIKR from foreign and domestic threats. HITRAC works in partnership with the U.S. Intelligence Community and national law enforcement to integrate and analyze intelligence and law enforcement information in threat and risk analysis products. HITRAC also works in partnership with the SSAs and owners and operators to ensure that their expertise on infrastructure operations is integrated into HITRAC analyses.

National Plan Coordination

Q: How does the NIPP relate to other national plans?
A: The NIPP outlines the overarching elements of the CIKR protection effort applicable within and across all sectors. The SSPs are an integral component of the NIPP and exist as independent documents to address the unique perspective, risk landscape, and

methodologies of each sector. In terms of incident management, the NIPP establishes the overall risk-based approach that defines the Nation's CIKR steady-state protective posture, while the National Response Framework and National Incident Management System provide the overarching framework, mechanisms, and protocols required for effective and efficient domestic incident management. The NIPP risk management framework, information-sharing network, and sector partnership model provide vital functions which inform and enable incident management decisions and activities.

Federal Grants

Q: Are grants available to help implement the NIPP?
A: Yes. Federal grants from DHS and other departments, as well as resources such as training and technical assistance, offer key support to State and local jurisdictions for CIKR protection programs. These grants and other programs provide avenues for directing Federal resources to meet CIKR needs based on risk that are more appropriately managed by State and local entities. DHS' FEMA/Grant Programs Directorate is responsible for coordinating Federal homeland security grant programs to help State, local, and tribal governments enhance their ability to prevent, protect against, respond to, and recover from terrorist acts or threats and other hazards. The Grant Programs Directorate offers State, local, and tribal partners access to significant funding through several grant programs that can be leveraged to support CIKR protection requirements based on risk and need. While States typically are the eligible applicants for DHS grant programs, certain private sector entities can apply directly for grant funds through programs such as the Port Security Grant Program and the Intercity Bus Security Program. For more information on the actual grant process, visit the Grant Programs Directorate website at http://www.fema.gov/government/grant/index.shtm.

CIKR Protection Outreach and Awareness

Q: What does DHS do to inform its partners about the NIPP and the SSPs?
A: DHS conducts an extensive outreach and awareness campaign to build sector and public awareness of the NIPP and the SSPs through various means, including speaking engagements, convention appearances, and distribution of printed and electronic materials. The NIPP web site, www.dhs.gov/nipp, provides direct links to the full version of the NIPP, those SSPs that can be widely disseminated, and supporting materials on the sectors and different elements of the NIPP. To discuss opportunities to participate in specific conferences, meetings, or events, or to request hard copies of selected materials, please contact NIPP@dhs.gov.

DHS also has an on-line educational course that provides an overview of the NIPP. This multimedia course is being updated to reflect the changes in the 2009 NIPP. Currently, the original course based on the 2006 NIPP can be found online at http://www.training.fema.gov/EMIWeb/IS/is860.asp.