Executive Summary

Protecting the critical infrastructure and key resources (CI/KR) of the United States is essential to the Nation's security, public health and safety, economic vitality, and way of life. Attacks on CI/KR could significantly disrupt the functioning of government and business alike and produce cascading effects far beyond the targeted sector and physical location of the incident. Direct terrorist attacks and natural, manmade, or technological hazards could produce catastrophic losses in terms of human casualties, property destruction, and economic effects, as well as profound damage to public morale and confidence. Attacks using components of the Nation's CI/KR as weapons of mass destruction could have even more devastating physical and psychological consequences.

1 Introduction

The overarching goal of the National Infrastructure Protection Plan (NIPP) is to:

> ***Build a safer, more secure, and more resilient America by enhancing protection of the Nation's CI/KR 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.***

The NIPP provides the unifying structure for the integration of existing and future CI/KR protection efforts into a single national program to achieve this goal. The NIPP framework will enable the prioritization of protection initiatives and investments across sectors to ensure that government and private sector resources are applied where they offer the most benefit for mitigating risk by lessening vulnerabilities, deterring threats, and minimizing the consequences of terrorist attacks and other manmade and natural disasters. The NIPP risk management framework recognizes and builds on existing protective programs and initiatives.

Protection includes actions to mitigate the overall risk to CI/KR 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 consequences associated with a terrorist attack or other incident (see figure S-1). Protection can include 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 programs, and implementing cyber security measures, among various others.

More information about the NIPP is available on the Internet at:
www.dhs.gov/nipp or by contacting DHS at: **nipp@dhs.gov**

Figure S-1: Protection

Achieving the NIPP goal requires actions to address a series of objectives that include:

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

These objectives require a collaborative partnership between and among a diverse set of security partners, including the Federal Government; State, Territorial, local, and tribal governments; the private sector; international entities; and nongovernmental organizations. The NIPP provides the framework that defines the processes and mechanisms that these security partners will use to develop and implement the national program to protect CI/KR across all sectors over the long term.

2 Authorities, Roles, and Responsibilities

The Homeland Security Act of 2002 provides the basis for Department of Homeland Security (DHS) responsibilities in the protection of the Nation's CI/KR. The act assigns DHS the responsibility to develop a comprehensive national plan for securing CI/KR and for recommending "measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other agencies of the Federal Government and in cooperation with State and local government agencies and authorities, the private sector, and other entities."

The national approach for CI/KR protection is provided through the unifying framework established in Homeland Security Presidential Directive 7 (HSPD-7). This directive establishes the U.S. policy for "enhancing protection of the Nation's CI/KR" and mandates a national plan to actuate that policy. In HSPD-7, the President designates the Secretary of Homeland Security as the "principal Federal official to lead CI/KR protection efforts among Federal departments and agencies, State and local governments, and the private sector" and assigns responsibility for CI/KR sectors to specific Sector-Specific Agencies (SSAs) (see table S-1). In accordance with HSPD-7, the NIPP delineates roles and responsibilities for security partners in carrying out CI/KR protection activities while respecting and integrating the authorities, jurisdictions, and prerogatives of these security partners.

Primary roles for CI/KR security partners include:

- **Department of Homeland Security:** Manage the Nation's overall CI/KR protection framework and oversee NIPP development and implementation.
- **Sector-Specific Agencies:** Implement the NIPP framework and guidance as tailored to the specific characteristics and risk landscapes of each of the CI/KR sectors designated in HSPD-7.
- **Other Federal Departments, Agencies, and Offices:** Implement specific CI/KR protection roles designated in HSPD-7 or other relevant statutes, executive orders, and policy directives.
- **State, Local, and Tribal Governments:** Develop and implement a CI/KR protection program as a component of their overarching homeland security programs.
- **Regional Partners:** Use partnerships that cross jurisdictional and sector boundaries to address CI/KR protection within a defined geographical area.
- **Boards, Commissions, Authorities, Councils, and Other Entities:** Perform regulatory, advisory, policy, or business oversight functions related to various aspects of CI/KR operations and protection within and across sectors and jurisdictions.
- **Private Sector Owners and Operators:** Undertake CI/KR protection, restoration, coordination, and cooperation activities, and provide advice, recommendations, and subject matter expertise to the Federal Government;
- **Homeland Security Advisory Councils:** Provide advice, recommendations, and expertise to the government regarding protection policy and activities.
- **Academia and Research Centers:** Provide CI/KR protection subject matter expertise, independent analysis, research and development (R&D), and educational programs.

Table S-1: Sector-Specific Agencies and HSPD-7 Assigned CI/KR Sectors

Sector-Specific Agency	Critical Infrastructure/Key Resources Sector
Department of Agriculture[1] Department of Health and Human Services[2]	Agriculture and Food
Department of Defense[3]	Defense Industrial Base
Department of Energy	Energy[4]
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	Drinking Water and Water Treatment Systems
Department of Homeland Security *Office of Infrastructure Protection*	Chemical Commercial Facilities Dams Emergency Services Commercial Nuclear Reactors, Materials, and Waste
Office of Cyber Security and Telecommunications	Information Technology Telecommunications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration, United States Coast Guard[5]	Transportation Systems[6]
Immigration and Customs Enforcement, Federal Protective Service	Government Facilities

[1] The Department of Agriculture is responsible for agriculture and food (meat, poultry, and egg products).

[2] The Department of Health and Human Services is responsible for food other than meat, poultry, and egg products.

[3] Nothing in this plan impairs or otherwise affects the authority of the Secretary of Defense over the Department of Defense (DOD), including the chain of command for military forces from the President as Commander in Chief, to the Secretary of Defense, to the commander of military forces, or military command and control procedures.

[4] The Energy Sector includes the production, refining, storage, and distribution of oil, gas, and electric power, except for commercial nuclear power facilities.

[5] The U.S. Coast Guard is the SSA for the maritime transportation mode.

[6] As stated in HSPD-7, the Department of Transportation and the Department of Homeland Security will collaborate on all matters relating to transportation security and transportation infrastructure protection.

3 The CI/KR Protection Program Strategy: Managing Risk

The cornerstone of the NIPP is its risk management framework (see figure S-2) that establishes the processes for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector risk. The risk management framework is structured to promote continuous improvement to enhance CI/KR protection by focusing activities on efforts to: set security goals; identify assets, systems, networks, and functions; assess risk based on consequences, vulnerabilities and threats; establish priorities based on risk assessments; implement protective programs; and measure effectiveness. The results of these processes drive CI/KR risk-reduction and risk management activities. The framework applies to the strategic threat environment that shapes program planning, as well as to specific threats or incident situations. DHS, the SSAs, and other security partners share responsibilities for implementing the risk management framework.

DHS, in collaboration with other security partners, measures the effectiveness of CI/KR protection efforts to provide constant feedback. This allows continuous refinement of the national CI/KR protection program in a dynamic process to efficiently achieve NIPP goals and objectives.

The risk management framework is tailored and applied on an asset, system, network, or function basis, depending on the fundamental characteristics of the individual CI/KR sectors. Sectors that are primarily dependent on fixed assets and physical facilities may use a bottom-up, asset-by-asset approach, while sectors (such as Telecommunications and Information Technology) with diverse and logical assets may use a top-down business or mission continuity approach. Each sector chooses the approach that produces the most actionable results for the sector and works with DHS to ensure that the relevant risk analysis procedures are compatible with the criteria established in the NIPP.

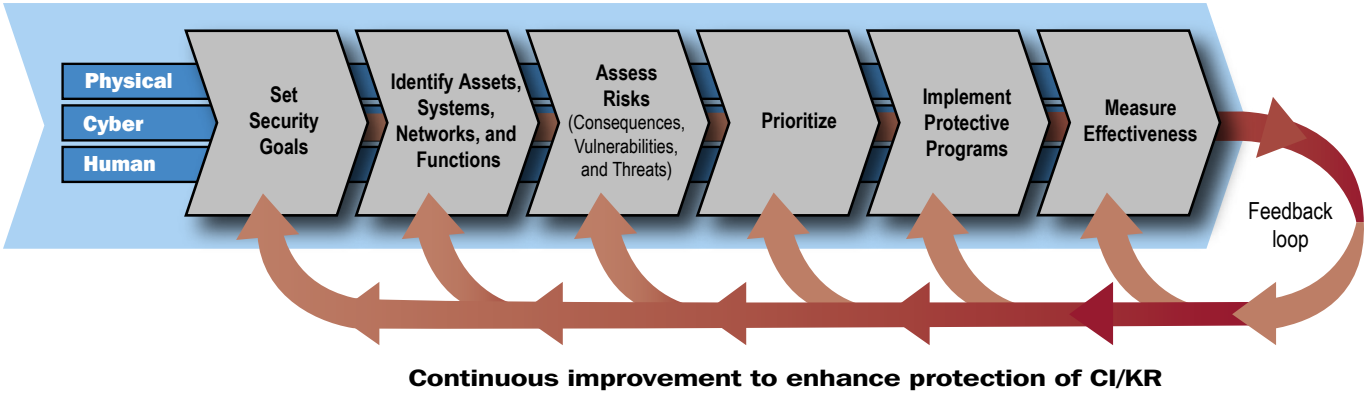
4 Organizing and Partnering for CI/KR Protection

The enormity and complexity of the Nation's CI/KR, the distributed character of its associated protective architecture, and the uncertain nature of the terrorist threat and other manmade and natural disasters make the effective implementation of protection efforts a great challenge. To be effective, the NIPP must be implemented using organizational structures and partnerships committed to sharing and protecting the information needed to achieve the NIPP goal and supporting objectives.

The NIPP defines the organizational structures that provide the framework for coordination of CI/KR protection efforts at all levels of government, as well as within and across sectors. Sector-specific planning and coordination are addressed through private sector and government coordinating councils that are established for each sector. Sector Coordinating Councils (SCCs) are comprised of private sector representatives. Government Coordinating Councils (GCCs) are comprised of representatives of the SSAs; other Federal departments and agencies; and State, local, and tribal governments. These councils create a structure through which representative groups from all levels of government and the private sector can collaborate or share existing consensus approaches to CI/KR protection.

DHS also works with cross-sector entities established to promote coordination, communications, and best practices sharing across CI/KR sectors, jurisdictions, or specifically defined

Figure S-2: NIPP Risk Management Framework



geographical areas. Cross-sector issues and interdependencies are addressed among the SCCs through the Partnership for Critical Infrastructure Security (PCIS). The PCIS membership is comprised of one or more members and their alternates from each of the SCCs. Cross-sector issues and interdependencies between the GCCs will be addressed through the Government Cross-Sector Council, which is comprised of the NIPP Federal Senior Leadership Council (FSLC), and the State, Local, and Tribal Government Cross-Sector Council (SLTGCC). Additionally, DHS may convene regionally based councils to address issues that cross jurisdictions or sectors, as required.

Efficient information-sharing and information-protection processes based on mutually beneficial, trusted relationships help to ensure implementation of effective, coordinated, and integrated CI/KR protective programs and activities. Information sharing enables both government and private sector partners to assess events accurately, formulate risk assessments, and determine appropriate courses of action. The NIPP uses a network approach to information sharing that represents a fundamental change in how security partners share and protect the information needed to analyze risk and make risk-based decisions. A network approach enables secure, multidirectional information sharing between and across government and industry. The network approach provides mechanisms, using information protection protocols as required, to support the development and sharing of strategic and specific threat assessments, threat warnings, incident reports, all-hazards impact assessments, and best practices. This information-sharing approach allows security partners to assess risks, conduct risk management activities, allocate resources, and make continuous improvements to the Nation's CI/KR protective posture.

NIPP implementation relies on critical infrastructure information provided by the private sector. Much of this is sensitive business or security information that could cause serious damage to private firms, the economy, public safety, or security through unauthorized disclosure or access. The Federal Government has a statutory responsibility to safeguard CI/KR protection-related information. DHS and other Federal agencies use a number of programs and procedures, such as the Protected Critical Infrastructure Information Program, to ensure that security-related information is properly safeguarded. Other relevant programs and procedures include Sensitive Security Information for transportation activities, Unclassified Controlled Nuclear Information, contractual provisions, classified national provisions, Classified National Security Information, Law Enforcement Sensitive Information, Federal Security Information Guidelines, Federal Security Classification Guidelines, and other requirements established by law.

The CI/KR protection activities defined in the NIPP are guided by legal requirements such as those described in the Privacy Act of 1974, and are designed to achieve a balance between an appropriate level of security and protection of civil rights and liberties.

5 CI/KR Protection: An Integral Part of the Homeland Security Mission

The Homeland Security Act; other statutes and executive orders; the National Strategies for Homeland Security, for the Physical Protection of CI/KR, and for Securing Cyberspace; and a series of Homeland Security Presidential directives—most importantly HSPD-7—collectively provide the authority for the component elements outlined in the NIPP. These documents work together to provide a coordinated national approach to homeland security that is based on a common framework for CI/KR protection, preparedness, and incident management.

The NIPP defines the CI/KR protection component of the homeland security mission. Implementing CI/KR protection requires partnerships, coordination, and collaboration among all levels of government and the private sector. To enable this, the NIPP provides guidance on the structure and content of each sector's CI/KR plan, as well as the CI/KR protection-related aspects of State and local homeland security plans. This provides a baseline framework that informs the tailored development, implementation, and updating of Sector-Specific Plans; State and local homeland security strategies; and security partner CI/KR protection programs.

To be effective, the NIPP must complement other plans designed to help prevent, prepare for, protect against, respond to, and recover from terrorist attacks, natural disasters, and other emergencies. Homeland security plans and strategies at the Federal, State, local, and tribal levels of government address CI/KR protection within their respective jurisdictions. Similarly, private sector owners and operators have responded to the post-9/11 environment by instituting a range of CI/KR protection-related plans and programs, including business continuity and resilience measures. Implementation of the NIPP will be fully coordinated between security partners to ensure that it does not result in the creation of duplicative or costly security requirements that offer little enhancement of CI/KR protection.

The NIPP and the National Response Plan (NRP) together provide a comprehensive, integrated approach to the homeland security mission. The NIPP establishes the overall risk-based approach that defines the Nation's CI/KR steady-state protective posture, while the NRP provides the approach for domestic incident management. Increases in CI/KR protective measures in the context of specific threats or that correspond to the threat conditions established in the Homeland Security Advisory System (HSAS) provide an important bridge between NIPP steady-state protection and incident management activities using the NRP.

The NRP is implemented to guide overall coordination of domestic incident management activities. NIPP partnerships and processes provide the foundation for the CI/KR dimension of the NRP, facilitating NRP threat and incident management across a spectrum of activities including incident prevention, response, restoration, and recovery.

6 Ensuring an Effective, Efficient Program Over the Long Term

To ensure an effective, efficient CI/KR protection program over the long term, the NIPP relies on the following mechanisms:

- **Building national awareness** to support the CI/KR protection program, related protection investments, and protection activities by ensuring a focused understanding of the all-hazards threat environment and of what is being done to protect and enable the timely restoration of the Nation's CI/KR in light of such threats;
- **Enabling education, training, and exercise programs** to ensure that skilled and knowledgeable professionals and experienced organizations are able to undertake NIPP-related responsibilities in the future;
- **Conducting R&D and using technology** to improve CI/KR protection-related capabilities or to lower the costs of existing capabilities so that security partners can afford to do more with limited budgets;
- **Developing, safeguarding, and maintaining data systems and simulations** to enable continuously refined risk assessment within and across sectors and to ensure preparedness for domestic incident management; and
- **Continuously improving the NIPP** and associated plans and programs through ongoing management and revision, as required.

7 Providing Resources for the CI/KR Protection Program

Chapter 7 describes an integrated, risk-based approach used to establish priorities, determine requirements, and fund the national CI/KR protection program; focus Federal grant assistance to State, local, and tribal entities; and complement relevant private sector activities. This integrated resource approach coordinates CI/KR protection programs and activities conducted by DHS, the SSAs, and other Federal entities, and focuses Federal grant funds to support national CI/KR protection efforts conducted at the State, local, and tribal levels. At the Federal level, DHS provides recommendations regarding CI/KR protection priorities and requirements to the Executive Office of the President through the National CI/KR Protection Annual Report. This report is based on information about priorities, requirements, and related program funding information that is submitted to DHS by the SSA of each sector, and assessed in the context of the National Risk Profile and national priorities. The process for allocating Federal resources through grants to State, local, and tribal governments uses a similar approach. DHS aggregates information regarding State, local, and tribal CI/KR protection priorities, requirements, and funding. DHS uses this data to inform the establishment of national priorities for CI/KR protection and to help ensure that funding is made available for protective programs that have the greatest potential for mitigating risk. This resource approach also includes mechanisms to involve private sector partners in the planning process, and supports collaboration among security partners to establish priorities, define requirements, share information, and maximize the use of finite resources.