National Infrastructure Protection Plan

Homeland Security

Building a Safer, More Secure, and More Resilient America

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; Federal Sector-Specific Agencies (SSAs); and other Federal, State, local, tribal, and private sector security partners. The NIPP provides the coordinated approach that will be used to establish national priorities, goals, and requirements for infrastructure protection 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 enhancing protection of the Nation's critical infrastructure and key resources (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.*

Achieving the Goal

Achieving the NIPP goal requires meeting a series of objectives that include understanding and sharing information about terrorist threats and other hazards, building security partnerships, implementing a long-term risk management program, and maximizing the efficient use of resources. Measuring progress toward achieving the NIPP goal requires that CI/KR security partners have:

- Coordinated risk-based CI/KR plans and programs in place addressing known and potential threats and hazards;
- Structures and processes that are flexible and adaptable to incorporate operational lessons learned and best practices and quickly adapt to a changing threat or incident environment;
- Processes in place to identify and address dependencies and interdependencies to allow for more timely and effective implementation of short-term protective actions and more rapid response and recovery; and
- Access to robust information-sharing networks that include relevant intelligence and threat analysis and real-time incident reporting.



The NIPP Value Proposition

The public-private partnership detailed in the NIPP provides the foundation for effective CI/KR protection, prevention, response, mitigation, and recovery. Government and private sector partners each bring core competencies that add value to the partnership and enhance the Nation's CI/KR protective posture.

Many industries justify their CI/KR protection efforts based on corporate business needs. Government can support these industry efforts and assist in broad-scale CI/KR protection through activities such as:

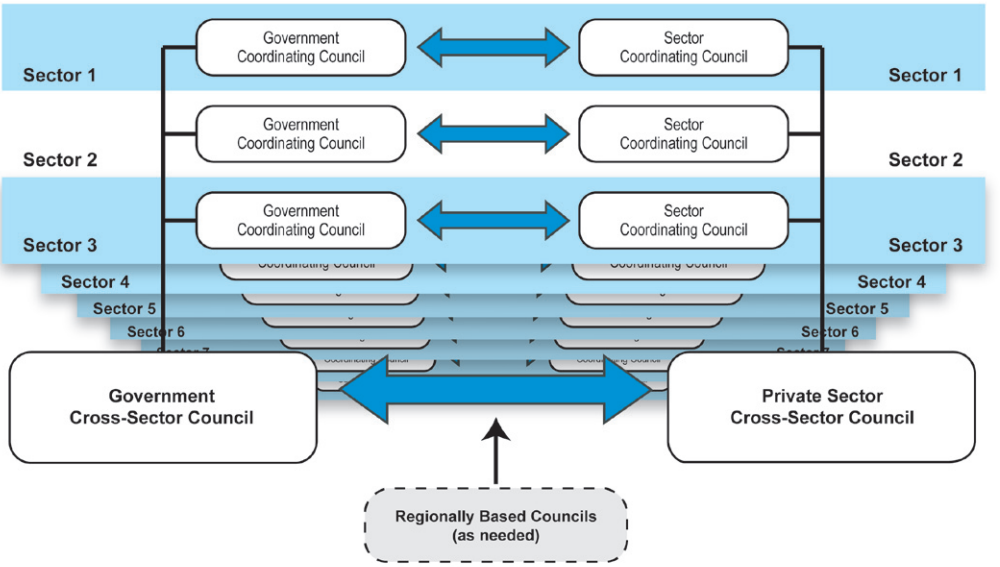
- Providing owners and operators with timely, analytical, accurate, and useful information on threats to CI/KR;
- Ensuring industry is engaged as early as possible in the development and enhancement of risk management activities, approaches, and actions;
- Ensuring industry is engaged as early as possible in the development and revision of Sector-Specific Plans (SSPs) and in planning and other CI/KR protection initiatives;
- Articulating to corporate leaders, publicly and privately, the business and national security benefits of investing in security measures that exceed individual business needs;
- Creating an environment that creates incentives and encourages companies to voluntarily adopt sound security practices;
- Working with industry to develop and prioritize key missions for each sector and enable their protection and/or restoration;
- Providing support for research needed to enhance CI/KR protection efforts; and
- Developing resources to engage in cross-sector interdependency studies through exercises, symposiums, training sessions, and computer modeling, which can enhance business continuity planning.

Sector Partnership Model

The enormity and complexity of the Nation's CI/KR, the diverse and dynamic nature of the actions required to protect CI/KR, and the uncertain nature of terrorist threats or disasters make the effective implementation of protection efforts challenging. To be effective, NIPP partners must be committed to sharing and protecting the information needed to achieve the NIPP goal and supporting objectives. DHS, in close collaboration with SSAs, is responsible for the overall coordination of the NIPP partnership and information-sharing network.

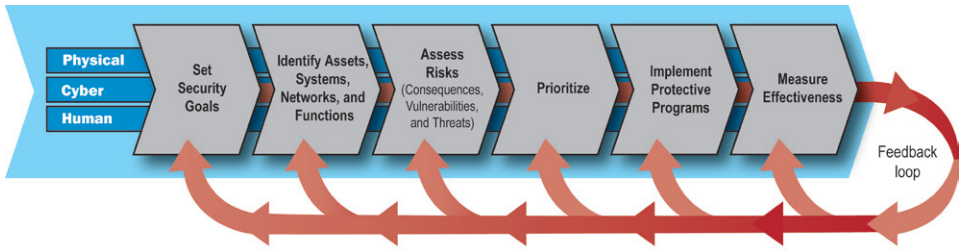
The structure through which representative groups from Federal, State, local, and tribal governments and the private sector can collaborate and develop consensus approaches to CI/KR protection consists of:

- The Private Sector Cross-Sector Council, made up of the Partnership for Critical Infrastructure Security;



- The Government Cross-Sector Council, made up of two subcouncils: the NIPP Federal Senior Leadership Council and the State, Local, and Tribal Government Coordinating Council;
- Individual Sector Coordinating Councils; and
- Government Coordinating Councils.

Risk Management Framework



Continuous improvement to enhance protection of CI/KR

The cornerstone of the NIPP is its risk management framework. This framework establishes the process for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector-specific risk that drives CI/KR-protection activities.

In the context of the NIPP, risk is the expected magnitude of loss (e.g., deaths, injuries, economic damage, loss of public confidence, or government capability) due to a terrorist attack, natural disaster, or other incident, along with the likelihood of such an event occurring and causing that loss.




The NIPP risk management framework includes the following activities:

- Set security goals: Define specific outcomes, conditions, end points, and/or performance targets that collectively constitute an effective protective posture.
- Identify assets, systems, networks, and functions: Develop an inventory of the assets, systems, and networks, including those located outside the United States, that comprise the Nation's CI/KR and the critical functionality therein; collect information pertinent to risk management that accounts for the fundamental characteristics of each sector.
- Assess risks: Determine risk by combining potential direct and indirect consequences of a terrorist attack or other hazards (including seasonal changes in consequences, dependencies and interdependencies associated with each identified asset, system, or network), known vulnerabilities to various potential attack vectors, and general or specific threat information.
- Prioritize: Aggregate and analyze risk assessment results to develop a comprehensive picture of asset, system, and network risk; establish priorities based on risk and determine protection and business continuity initiatives that provide the greatest mitigation of risk.
- Implement protective programs: Select sector-appropriate protective actions or programs to reduce or manage the risk identified; secure the resources needed to address priorities.
- Measure effectiveness: Use metrics and other evaluation procedures at the national and sector levels to measure progress and assess the effectiveness of the national CI/KR protection program in improving protection, managing risk, and increasing resiliency.

CI/KR protection is an ongoing and complex process. The NIPP provides the framework for the unprecedented cooperation needed to develop, implement, and maintain a coordinated national effort. The NIPP relies on supporting SSPs for full implementation of this framework throughout each CI/KR sector. SSPs are developed by the designated Federal SSAs in close collaboration with sector security partners.

Homeland Security

For questions or more information, please contact NIPP@dhs.gov or visit www.dhs.gov/nipp.

2006