

# 1. Introduction

Protecting and ensuring the continuity of 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. CI/KR include the assets, systems, networks, and functions that provide vital services to the Nation. Terrorist attacks on CI/KR and other manmade or natural disasters could significantly disrupt the functioning of government and business alike, and produce cascading effects far beyond the affected CI/KR and physical location of the incident. Direct and indirect impacts could result in large-scale human casualties, property destruction, and economic disruption, and also significantly damage national morale and public confidence. Terrorist attacks using components of the Nation’s CI/KR as weapons of mass destruction (WMD)<sup>7</sup> could have even more devastating physical, psychological, and economic consequences.

The protection of the Nation’s CI/KR is essential for 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 physical, cyber, and human CI/KR assets, systems, networks, functions, or their interconnecting links resulting from exposure, injury, destruction, incapacitation, or exploitation. In the context of the National Infrastructure Protection Plan (NIPP), this includes actions to deter the threat, mitigate vulnerabilities, or minimize consequences associated with a terrorist attack or other incident (see figure 1-1). Protection can include a wide range of activities such as improving business protocols, hardening facilities, building resiliency and redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing security systems, leveraging “self-healing” technologies, promoting workforce surety programs, or implementing cyber security measures, among various others. The NIPP and its complementary Sector-Specific Plans (SSPs) provide a consistent, unifying structure for integrating both existing and future CI/KR protection efforts. The NIPP also

Figure 1-1: Protection



<sup>7</sup> (1) Any explosive, incendiary, or poison gas (i) bomb, (ii) grenade, (iii) rocket having a propellant charge of more than 4 ounces, (iv) missile having an explosive or incendiary charge of more than one-quarter ounce, or (v) mine or (vi) similar device; (2) any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors; (3) any weapon involving a disease organism; or (4) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life (18 U.S.C. 2332a).

provides the core processes and mechanisms that enable all levels of government and private sector security partners to work together to implement CI/KR protection in an effective and efficient manner.

The NIPP was developed through extensive coordination with security partners at all levels of government and the private sector. NIPP processes are designed to be adapted and tailored to individual sector and security partner requirements. Participation in the implementation of the NIPP provides the government and the private sector the opportunity to use collective expertise and experience to more clearly define CI/KR protection issues and practical solutions, and to ensure that existing CI/KR protection approaches and efforts, including business continuity and resiliency planning, are recognized.

## 1.1 Purpose

CI/KR protection is an ongoing process with multiple intersecting elements. The NIPP provides the framework for the unprecedented cooperation that is needed to develop, implement, and maintain a coordinated national effort that brings together government at all levels, the private sector, and nongovernmental organizations and international allies. The NIPP depends on supporting SSPs for full implementation of this framework throughout each CI/KR sector. SSPs are developed by the designated Federal Sector-Specific Agencies (SSAs) in close collaboration with sector security partners.

Together, the NIPP and SSPs provide the mechanisms for identifying critical assets, systems, networks, and functions; understanding threats; assessing vulnerabilities and consequences; prioritizing protection initiatives and investments based on costs and benefits so that they are applied where they offer the greatest mitigation of risk; and enhancing information-sharing mechanisms and protective measures within and across CI/KR sectors. The NIPP and SSPs will evolve in accordance with changes to the Nation's CI/KR and the threat environment, as well as evolving strategies and technologies for protecting against and responding to threats and incidents.

## 1.2 Scope

The NIPP considers a full range of physical, cyber, and human security elements within and across all of the Nation's CI/KR

sectors. 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 an augmented focus on the protection of CI/KR from the unique and potentially catastrophic impacts of terrorist attacks. At the same time, the NIPP 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.

The NIPP addresses ongoing and future activities within each of the CI/KR sectors identified in HSPD-7 and across the sectors regionally and nationally. It defines processes and mechanisms used to prioritize protection of U.S. CI/KR (including Territories and territorial seas) and to address the interconnected global networks upon which the Nation's CI/KR depend. The processes outlined in the NIPP and the SSPs recognize that protective measures do not end at a facility's fence line or at a national border, and are often a component of a larger business continuity approach. Also considered are the implications of cross-border infrastructures, international vulnerabilities, and cross-sector dependencies and interdependencies.

## 1.3 Applicability

While the NIPP covers the full range of CI/KR sectors as defined in HSPD-7, it is applicable to the various public and private sector security partners in different ways. The framework generally is applicable to all security partners with CI/KR protection responsibilities and includes explicit roles and responsibilities for the Federal Government, including CI/KR under the control of independent regulatory agencies, and the legislative, executive, or judicial branches. Federal departments and agencies with specific responsibilities for CI/KR protection are required to take actions consistent with HSPD-7. The NIPP also provides an organizational structure, protection guidelines, and recommended activities for other security partners to help ensure consistent implementation of the national framework and the most effective use of resources. State,<sup>8</sup> local,<sup>9</sup> and tribal government security partners are required to establish CI/KR protection programs consistent with the National Preparedness Goal and as a condition of eligibility for certain Federal grant programs.

<sup>8</sup> Consistent with the definition of "State" in the Homeland Security Act of 2002, all references to States within the NIPP are applicable to Territories and include by reference any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States (Homeland Security Act).

<sup>9</sup> A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government; an Indian tribe or authorized tribal organization, or, in Alaska, a Native village or Alaska Regional Native Corporation; and a rural community, unincorporated town or village, or other public entity (Homeland Security Act).

Private sector owners and operators are encouraged to participate in the NIPP partnership model and to initiate protective measures to augment existing plans for risk management, business continuity, and incident management and emergency response in line with the NIPP framework.

### 1.3.1 Goal

The overarching goal of the 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.*

Achieving this 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 both to incorporate operational lessons learned and best practices and also to 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.

### 1.3.2 The Value Proposition

The public-private partnership called for in the NIPP provides the foundation for effective CI/KR protection. A wide range of government and private sector partners bring core competencies that add value to the partnership. Prevention, response, mitigation, and recovery efforts are most efficient and effective when there is full participation of government and industry partners and the efforts suffer without the full participation of either partner.

The success of the partnership depends on articulating the mutual benefits to government and private sector partners. While articulating the value proposition to the government typically is clear, it is often more difficult to articulate the direct benefits of participation for the private sector. Industry provides the following capabilities, outside of government core competencies:

- Ownership and management of a vast majority of CI/KR in most sectors;
- Visibility into CI/KR assets, networks, facilities, functions, and other capabilities;
- Ability to take initial actions to respond to incidents;
- Ability to innovate and to provide products, services, and technologies to quickly focus on requirements; and
- Existing robust mechanisms useful for sharing and protecting sensitive information regarding threats, vulnerabilities, countermeasures, and best practices.

In assessing the value proposition for the private sector, there is a clear national security and homeland security interest in ensuring the collective protection of the Nation's CI/KR. Government can encourage industry to go beyond efforts already justified by their corporate business needs to assist in broad-scale CI/KR protection through activities such as:

- Providing owners and operators timely, analytical, accurate, and useful information on threats to CI/KR;
- Ensuring industry is engaged as early as possible in the development of initiatives and policies related to NIPP implementation and, as needed, revision of the NIPP Base Plan;
- Ensuring industry is engaged as early as possible in the development and revision of the SSPs and in planning and other CI/KR protection initiatives;
- Articulating to corporate leaders, through the use of public platforms and private communications, both the business and national security benefits of investing in security measures that exceed their business case;
- 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 CI/KR protection efforts;

- Developing the resources to engage in cross-sector interdependency studies, through exercises, symposiums, training sessions, and computer modeling, that result in guided decision support for business continuity planning; and
- Enabling time-sensitive information sharing and restoration and recovery support to priority CI/KR facilities and services during incidents in accordance with the provisions of the Robert T. Stafford Disaster Relief and Emergency Assistance Act.

The above examples illustrate some of the ways in which the government can, by actively partnering with the private sector, add value to industry's ability to assess its own risk and refine its business continuity and security plans, as well as contribute to the security and economic vitality of the Nation. The NIPP outlines the high-level value in the overall public-private partnership for CI/KR protection. The SSPs will outline specific future activities and initiatives that articulate the corresponding value to those sector-specific CI/KR partnerships and protection activities.

## 1.4 Threats to the Nation's CI/KR

Presidential guidance and national strategies focus CI/KR protection efforts on addressing the emerging terrorist threat environment as an essential component of the all-hazards nature of the homeland security mission. The emergence of the terrorist threat as a reality in the 21<sup>st</sup> century presents new challenges and requires new approaches focused on intelligence-driven analyses, information sharing, and unprecedented partnerships between the government and the private sector at all levels. As a result of decades of experience responding to natural disasters, industrial accidents, and the deliberate acts of malicious individuals, the Nation's CI/KR owners and operators have adapted methods for preventing, mitigating, and responding to these incidents as a matter of business continuity. However, government and business continuity, incident, and emergency response plans and preparedness efforts must continue to adapt to a changing threat and hazard environment, and continually address vulnerabilities and gaps in CI/KR protection.

### 1.4.1 The Vulnerability of the U.S. Infrastructure to 21<sup>st</sup> Century Threats

America is an open, technologically sophisticated, highly interconnected, and complex Nation with a wide array of infrastructure that spans important aspects of U.S. Government, economy, and society. The majority of the CI/KR-related assets, systems, and networks are owned and

operated by the private sector. In some sectors, however, such as Water and Government Facilities, the majority of owners and operators are government or quasi-governmental entities. The great diversity and redundancy of the Nation's CI/KR provide for significant physical and economic resilience in the face of terrorist attacks, natural disasters, or other emergencies, and contribute to the unprecedented strength of the Nation's economy. However, this vast and diverse aggregation of highly interconnected assets, systems, and networks may also present an attractive array of targets to terrorists and magnify greatly the potential for cascading failure in the wake of catastrophic natural or manmade disasters. Improvements in protection focusing on prioritized elements of CI/KR deemed nationally critical through implementation of the NIPP can make it more difficult for terrorists to launch attacks and lessen the impacts of any attack or other disaster that does occur.

### 1.4.2 The Nature of Possible Terrorist Attacks

The number and high profile of international and domestic terrorist attacks during the last decade underscore the determination and persistence of terrorist organizations. Extremist organizations have proven to be relentless, patient, opportunistic, and flexible, learning from experience and modifying tactics and targets to exploit perceived vulnerabilities and avoid observed strengths. Current analysis of terrorist goals and motivations points to domestic and international CI/KR as potentially prime targets for terrorist attacks. As security measures around more predictable targets increase, terrorists are likely to shift their focus to less protected targets. Enhancing countermeasures to address any one terrorist tactic or target may increase the likelihood that terrorists will shift to another.

Terrorist organizations have shown an understanding of the potential consequences of carefully planned attacks on economic, transportation, and symbolic targets both within the United States and abroad. Future terrorist attacks against CI/KR across the United States could seriously threaten national security, result in mass casualties, weaken the economy, and damage public morale and confidence.

The NIPP considers a broad range of terrorist objectives, intentions, and capabilities to assess the threat to various components of the Nation's CI/KR. Based on that assessment, terrorists may contemplate attacks against the Nation's CI/KR to achieve three general types of effects:

- **Direct Infrastructure Effects:** Disruption or arrest of critical functions through direct attacks on an asset, system, or network.

- **Indirect Infrastructure Effects:** Cascading disruption and financial consequences for the government, society, and economy through public and private sector reactions to an attack. An operation could reflect an appreciation of interdependencies between different elements of CI/KR, as well as the psychological importance of demonstrating the ability to strike effectively inside the United States.
- **Exploitation of Infrastructure:** Exploitation of elements of a particular infrastructure to disrupt or destroy another target or produce cascading consequences. Attacks using CI/KR elements as a weapon to strike other targets, allowing terrorist organizations to magnify their capabilities far beyond what could be achieved using their own limited resources.

The NIPP outlines the ways in which the Department of Homeland Security (DHS) and its security partners use threat analysis to inform comprehensive risk assessments and risk-mitigation activities. The risk management framework discussed in chapter 3 strikes a balance between ways to mitigate specific and general threats. It ensures that the range of plausible attack scenarios considered is broad enough to avoid a “failure of imagination,” yet contains sufficient detail to enable quantitative and qualitative risk assessment and definable actions and programs to enhance resiliency, reduce vulnerabilities, deter threats, and mitigate potential consequences.

## 1.5 All-Hazards and CI/KR Protection

In addition to addressing CI/KR protection related to terrorist threats, the NIPP also describes activities relevant to CI/KR protection and preparedness in an all-hazards context. The direct impacts, disruptions, and cascading effects of natural disasters (e.g., Hurricanes Katrina and Rita, the Northridge earthquake, etc.) and manmade incidents (e.g., the Three Mile Island Nuclear Power Plant accident or the Exxon Valdez oil spill) on the Nation’s CI/KR are well documented. The recent experience in the wake of Hurricane Katrina, for example, underscored the vulnerabilities and interdependencies of the Nation’s CI/KR.

Many owners and operators, government emergency managers, and first-responders have developed strategies, plans, policies, and procedures to prepare for, mitigate, respond to, and recover from a variety of natural and manmade incidents. The NIPP framework recognizes these efforts and provides an augmented focus on the protection of America’s CI/KR against terrorist attacks. In fact, the day-to-day public-private coordination structures, information-sharing network, and risk management framework used to implement NIPP

steady-state CI/KR protection efforts continue to function and provide the CI/KR protection dimension for incident management activities under the National Response Plan (NRP). The NIPP, and the public and private sector partnership that it represents, works in conjunction with other plans and initiatives to provide a stronger foundation for preparedness in an all-hazards context. NIPP elements include:

- A comprehensive approach that integrates authorities, capabilities, and resources on a national, regional, and local scale;
- A complete and accurate assessment of the Nation’s CI/KR that not only helps inform the prioritization of protection activities, but also enables response and recovery efforts;
- An organization and coordinating structure to enable effective partnership between and among Federal, State, local, and tribal governments, regional and international entities, as well as the private sector;
- An integrated approach to enhancing protection of the physical, cyber, and human elements of the Nation’s CI/KR in which individual security measures complement one another; and
- The development and use of sophisticated analytical and modeling tools to help inform effective risk-mitigation programs in an all-hazards context.

## 1.6 Planning Assumptions

The NIPP is based on the following planning assumptions that relate to the sector-specific and cross-sector nature of the CI/KR protection mission, the adaptive nature of the terrorist threat, and the most effective approaches to all-hazards CI/KR protection.

### 1.6.1 Sector-Specific Nature of CI/KR Protection

- Approaches to CI/KR protection and risk management vary based on sector business characteristics, risk landscape, protection authorities, requirements, and maturity;
- Assets, systems, and networks vary in criticality within and across CI/KR sectors;
- Successful CI/KR protection requires robust baseline information on assets, systems, networks, and functions within and across CI/KR sectors, regions,<sup>10</sup> and specific localities;
- Owners and operators conduct risk management planning and invest in security from a business perspective and may

<sup>10</sup> Areas with shared geography, economies, or other characteristics that can serve as the focal points for CI/KR protection through public and private partnerships.

look for various types of incentives to elicit maximum participation in CI/KR protection;

- In some sectors, private firms own the vast majority of CI/KR;
- Some regulatory agencies may already impose protective measure requirements on private sector owners and operators. Coordination between the private sector, DHS, and the SSAs is required to address measures for threats beyond the regulatory baseline; and
- Strong relationships among security partners are essential to meet the overarching goal and supporting objectives set forth in the NIPP.

### 1.6.2 Cross-Sector Dependencies and Interdependencies

- In some cases, a failure in one sector may significantly impact another sector's ability to perform necessary and critical functions; and
- Many CI/KR sectors rely on the service grids of the Energy, Information Technology, Telecommunications, and Transportation sectors. Failures in these sectors can prevent others from functioning properly. Relevant sector dependencies and interdependencies must be considered when developing SSPs.

### 1.6.3 Adaptive Nature of the Terrorist Threat

- CI/KR protection activities take place in a highly dynamic threat environment. The general threat environment changes as the capabilities and the intentions of terrorists evolve;
- It is not practical or feasible to protect all assets, systems, and networks against every possible terrorist attack vector. A risk-based approach enhanced by intelligence and information analysis and reporting provides the basis for an effective risk management strategy and efficient resource allocation;
- CI/KR protection planning at the national and sector levels must address the full range of plausible threats and hazards, not just those most frequently reported or considered to be the most likely to occur; and
- A proactive approach is required to enhance decision-making processes, provide advance warning to potentially targeted or vulnerable CI/KR, and assist owners and operators in taking protective steps to enhance CI/KR protection in an all-hazards context.

### 1.6.4 All-Hazards Nature of CI/KR Protection

- Natural disasters such as floods, hurricanes, tornadoes, wildfires, pandemics, and earthquakes, and unintentional manmade disasters such as oil spills or radiological accidents, also pose a threat to the Nation's CI/KR; and
- Efforts to enhance the protection of CI/KR from terrorist attacks should support all-hazards preparedness and response whenever possible.

## 1.7 Special Considerations

CI/KR protection planning involves special consideration for protection of sensitive infrastructure information, the unique cyber and human elements of infrastructure, and complex international relationships.

**Assets, systems, and networks include one or more of the following elements:**

**Physical**—tangible property;

**Cyber**—electronic information and communications systems, and the information contained therein; and

**Human**—critical knowledge of functions or people uniquely susceptible to attack.

### 1.7.1 Protection of Sensitive Information

**Protection of sensitive information involves:**

- **Protection** from unauthorized access and public disclosure;
  - **Security** to guard against damage, theft, modification, or exploitation (e.g., firewalls, physical security); and
  - **Detection** to identify malicious activity affecting an electronic information or communications system.
- Partnership with the private sector requires the establishment of mutually beneficial, trusted relationships supported by a network approach to providing access to information and a business continuity approach to minimizing or managing risk;
  - Great care must be taken by the government to ensure that sensitive infrastructure information is protected and used appropriately to enhance the protection of the Nation's CI/KR;

- Information on specific industry assets and vulnerabilities is particularly sensitive because public release may lead to breaches in security, competitive advantage, and/or adverse impacts on an industry’s position in the marketplace; and
- DHS does not have broad regulatory authority over CI/KR and cannot compel private sector entities to submit infrastructure or operational information. Rather, DHS works in partnership with industry and the SSAs to identify the necessary information and promote the trusted exchange of such data.

### 1.7.2 The Cyber Dimension

**Cyber infrastructure** includes electronic information and communications systems, and the information contained in those systems. Computer systems, control systems such as Supervisory Control and Data Acquisition (SCADA) systems, and networks such as the Internet are all part of cyber infrastructure.

**Information and communications systems** are composed of hardware and software that process, store, and communicate. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information.

- The U.S. economy and national security are highly dependent upon the global cyber infrastructure. Cyber infrastructure enables all sectors’ functions and services, resulting in a highly interconnected and interdependent global network of CI/KR;
- A spectrum of malicious actors could conduct attacks against the cyber infrastructure using cyber attack tools. Because of the interconnected nature of the cyber infrastructure, these attacks could spread quickly and have a debilitating impact;
- The use of innovative technology and interconnected networks in operations improves productivity and efficiency, but also increases the Nation’s risk to cyber threats if cyber security is not addressed and integrated appropriately;
- The interconnected and interdependent nature of the Nation’s CI/KR makes it problematic to address the protection of physical and cyber assets independently;

- Cyber security includes preventing damage to, unauthorized use of, or exploitation of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. Cyber security also includes restoring electronic information and communications systems in the event of a terrorist attack or natural disaster; and
- The NIPP addresses reducing cyber risk and enhancing cyber security in two ways: (1) as a cross-sector cyber element that involves DHS, SSAs, and private sector owners and operators; and (2) as a major component of the Information Technology sector’s responsibility in partnership with the Telecommunications sector.

### 1.7.3 The Human Element

- The NIPP recognizes that each CI/KR asset, system, and network is made up of physical and cyber components, and human elements;
- The human element requires:
  - Identifying and preventing the insider threat resulting from infiltration or individual employees determined to do harm;
  - Identifying, protecting, and supporting (e.g., via cross-training) employees and other persons with critical knowledge or functions; and
  - Identifying and mitigating fear tactics used by terrorist agents and disaffected insiders;
- Assessing human element vulnerabilities is more subjective than assessing the physical or cyber vulnerabilities of corresponding assets, systems, and networks; and
- Diverse protective programs and actions to address threats posed by employees and to employees need to be put into place across all sectors.

### 1.7.4 International CI/KR Protection

- The NIPP addresses international CI/KR protection, including interdependencies and vulnerabilities based on threats that originate outside the country or transit through it;
- The Federal Government and the private sector work with foreign governments and international/multinational organizations to enhance the confidentiality, integrity, and availability of cyber infrastructure and products;

- Protection of assets, systems, and networks that operate across or near the borders with Canada and Mexico, or rely on other international aspects to enable critical functionality, requires coordination with, and planning and/or sharing resources among, neighboring governments at all levels, as well as private sector CI/KR owners and operators;
- The Federal Government and private sector corporations have a significant number of facilities located outside the United States that may be considered CI/KR;
- Special consideration is required when CI/KR is extensively integrated into an international or global market (e.g., financial services, agriculture, energy, transportation, telecommunications, or information technology) or when a sector relies on inputs that are not within the control of U.S. entities; and
- Special consideration is required when government facilities and functions are directly affected by foreign-owned and -operated commercial facilities.

## 1.8 Achieving the Goal of the NIPP

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 security partnerships to share information and implement CI/KR protection programs;
- Implementing a long-term risk management program that includes:
  - Hardening and ensuring the resiliency of CI/KR 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 CI/KR disruptions to limit the impacts on public health and safety, the economy, and government functions; and
  - Planning for rapid CI/KR restoration and recovery for those events that are not preventable; and
- Maximizing efficient use of resources for CI/KR protection.

This section provides a summary of the actions needed to address these objectives. More detailed discussions of these actions are included in the chapters that follow.

### 1.8.1 Understanding and Sharing Information

One of the essential elements needed to achieve the Nation's CI/KR protection goals is to ensure the availability and flow of accurate, timely, and relevant information and/or intelligence about terrorist threats and other hazards, information analysis, and incident reporting. This includes actions to:

- Establish effective information-sharing processes and protocols among security partners;
- Provide intelligence and information to SSAs and other CI/KR sector partners as permitted by law;
- Analyze, warehouse, and share risk assessment data in a secure manner consistent with relevant legal requirements and information protection responsibilities;
- Provide protocols for real-time threat and incident reporting, alert, and warning; and
- Provide protocols for the protection of sensitive information.

Chapter 3 details the threat analysis process and products aimed at better understanding and characterizing terrorist threats. Chapter 4 describes the NIPP network approach to information sharing and the process for protecting sensitive CI/KR-related information.

### 1.8.2 Building Security Partnerships

Building security partnerships represents the foundation of the national CI/KR protection effort. These partnerships provide a framework to:

- Exchange ideas, approaches, and best practices;
- Facilitate security planning and resource allocation;
- Establish effective coordinating structures among security partners;
- Enhance coordination with the international community; and
- Build public awareness.

Chapters 2 and 4 detail security partner roles and responsibilities related to CI/KR protection, as well as specific mechanisms for governance, coordination, and information sharing necessary to enable effective partnerships.

### 1.8.3 Implementing a Long-Term CI/KR Risk Management Program

The long-term risk management program detailed in the NIPP includes processes to:

- Establish a risk management framework to guide CI/KR protection programs and activities;
- Identify and regularly update the status of CI/KR protection programs within and across sectors;
- Conduct and update risk assessments at the asset, system, network, sector, cross-sector, regional, national, and international levels;
- Develop and deploy new technologies to enable more effective and efficient CI/KR protection; and
- Provide a system for continuous measurement and improvement of CI/KR protection, including:
  - Establishing performance metrics to assess the effectiveness of protective programs; and
  - Updating the NIPP and SSPs as required.

The NIPP also specifies the processes, key initiatives, and milestones necessary to implement an effective long-term CI/KR risk management program. Chapter 3 provides details regarding the NIPP risk management framework; chapter 6 addresses issues important for sustaining and improving CI/KR protection over the long term.

### 1.8.4 Maximizing Efficient Use of Resources for CI/KR Protection

Maximizing the efficient use of resources for CI/KR protection includes a coordinated and integrated annual process for program implementation that:

- Supports prioritization of programs and activities within and across sectors;
- Informs the annual Federal process regarding planning, programming, and budgeting for national-level CI/KR protection;
- Helps to align the resources of the Federal budget to the CI/KR protection mission and goals, and to enable tracking and accountability for the expenditure of public funds;

- Takes into account State, local, and tribal government and private sector considerations related to planning, programming, and budgeting;
- Draws on expertise across organizational and national boundaries;
- Shares expertise and speeds implementation of best practices;
- Recognizes the need to build a business case based on the NIPP value proposition for further private sector CI/KR protection investments; and
- Identifies potential incentives for security-related activities where they do not naturally exist in the marketplace.

Chapter 5 explains how a coordinated national approach to the CI/KR protection mission enables the efficient use of resources. Efficient use of resources requires a deliberate process to continuously improve the technology, databases, data systems, and other approaches used to protect CI/KR and manage risk. These processes are detailed in chapter 6. Chapter 7 describes the annual processes required to establish investment mechanisms for CI/KR protection that reflect appropriate coordination with SSAs and other security partners regarding resource prioritization and allocation. Also discussed are processes to utilize grants and other funding authorities to maximize and focus the use of resources to support program priorities.

**More information about the NIPP is available on the Internet at: [www.dhs.gov/nipp](http://www.dhs.gov/nipp) or by contacting DHS at: [nipp@dhs.gov](mailto:nipp@dhs.gov)**

