



# Interim National Infrastructure Protection Plan

February 2005



Homeland  
Security



# Interim National Infrastructure Protection Plan

February 2005

## Contents

<b>1 Introduction</b>	<b>1</b>
1.1 Purpose of the Interim NIPP	1
1.2 Organization and Scope	2
1.3 Definitions	3
1.4 Key Stakeholders and Partnerships	4
1.5 Next Steps	5
<b>2 National Goals, Framework, and Actions</b>	<b>7</b>
2.1 Goals and Objectives	7
2.2 NIPP Risk Management Framework	8
2.2.1 Five-Step Process	9
2.2.2 Two-Pronged Implementation	10
2.3 Core Actions	10
<b>3 Vulnerability Reduction Program</b>	<b>12</b>
3.1 Identify CI/KR	14
3.1.1 Sector-Specific Inventories	14

3.1.2 National CI/KR Inventory	16
3.1.3 Updating and Using the Inventories	16
3.2 Identify and Assess Vulnerabilities	17
3.3 Analyze, Normalize, and Prioritize CI/KR	19
3.3.1 Analysis and Prioritization Process	19
3.3.2 Interdependencies Analysis	20
3.4 Develop and Implement Protective Programs for CI/KR	20
3.5 Measure Effectiveness	22
3.6 Continuous Improvement	24
<b>4 Threat-Initiated Actions</b>	<b>25</b>
4.1 Identify CI/KR	26
4.2 Identify and Assess Vulnerabilities	27
4.3 Analyze, Normalize, and Prioritize CI/KR	27
4.4 Develop and Implement Protective Programs for CI/KR	27
4.5 Measure Effectiveness	28
4.6 Continuous Improvement	28
<b>5 Roles and Responsibilities</b>	<b>29</b>
5.1 Key Responsibilities	29
5.1.1 Department of Homeland Security	29
5.1.2 Sector-Specific Agencies	32
5.1.3 The Private Sector	33
5.1.4 State, Local, and Tribal Entities	34
5.1.5 Other Federal Agencies	34
5.2 Leadership and Coordination Mechanisms	34
5.2.1 NIPP Leadership Councils	35
5.2.2 Sector Coordinating Councils	36
5.2.3 Government Coordinating Councils	36
5.2.4 Coordination Support Mechanisms	36
5.2.5 State, Local, and Tribal Government Coordination	37
<b>6 Integration with Other Plans</b>	<b>38</b>
6.1 National Response Plan (NRP)	38
6.2 National Incident Management System (NIMS)	39
6.3 Other HSPD-7 Requirements	39
6.3.1 SSA Annual Plans	39
6.3.2 Internal Federal Plans	40

6.3.3 Research and Development Plan	40
6.3.4 Other Department and Agency Infrastructure Protection-Related Plans	42
6.4 International Agreements	42
List of Acronyms	43

## List of Exhibits

Exhibit 1: Sector-Specific Agencies and Assigned Sectors	3
Exhibit 2: NIPP Goals and Objectives	7
Exhibit 3: CIP Risk Management Framework	9
Exhibit 4: Benefits of Risk Management Framework	10
Exhibit 5: Vulnerability Reduction Program	12
Exhibit 6: Protection of Critical Infrastructure Information	14
Exhibit 7: Core Metrics	23
Exhibit 8: Threat-Initiated Actions	25
Exhibit 9: Key Roles and Responsibilities by Risk Management Framework Stage	30
Exhibit 10: Organization of Coordinating Councils	35



# 1. Introduction

Protecting our Nation's critical infrastructure and key resources (CI/KR) is vital to our national security, economic vitality, and way of life. Attacks on critical infrastructure could disrupt the direct functioning of key business and government activities, facilities, and systems, as well as have cascading effects throughout the Nation's economy and society. Furthermore, direct attacks on individual key assets could result not only in large-scale human casualties and property destruction, but also in profound damage to national prestige, morale, and confidence.

To provide a consistent, unifying structure for integrating critical infrastructure protection (CIP) efforts into a national program, the Department of Homeland Security (DHS) is developing the National Infrastructure Protection Plan (NIPP). Development of the NIPP is an ongoing, evolving process that requires the participation of all stakeholders from the private sector, State, local, and tribal entities, and the Federal Government. The NIPP outlines how DHS and its stakeholders will develop and implement

the national effort to protect infrastructures across all sectors. As these CIP efforts are developed, implemented, and refined, the NIPP will be updated to reflect this progress.

The national CIP program will be an ongoing effort to protect the Nation's CI/KR. As one of the initial steps in this program, DHS and the Sector-Specific Agencies (SSAs) will share and discuss this NIPP with critical stakeholders to further ensure its effectiveness and success. Stakeholder perspectives are essential for a comprehensive NIPP supported by effective Sector-Specific Plans (SSPs) that will detail the application of the risk management framework to each of the 17 sectors. As such, the SSAs will work with their stakeholders to develop and implement the SSPs, so that protective programs and limited public and private resources are targeted toward the most critical assets within and across sectors. Success will be achieved by working together through public and private sector partnerships to identify, prioritize, and protect the Nation's CI/KR.

## 1.1 Purpose of the NIPP

The events of September 11, 2001 demonstrated our Nation's vulnerability to terrorist attacks. Protection of CI/KR requires knowledge of terrorist tactics and targets, combined with a comprehensive understanding of CI/KR

vulnerabilities and the protective measures that can effectively eliminate or mitigate those vulnerabilities. However, even with all of the resources of the United States, it is not possible to protect all assets against every possible type of terrorist attack. The Nation's CIP program must prioritize protection across sectors, so that resources are applied where they offer the most benefit for reducing vulnerability, deterring threats, and minimizing consequences of attacks. This is an effort that requires the integrated, coordinated support of Federal departments and agencies; State, local, and tribal entities; and public and private sector asset owners and operators.

The Interim NIPP is based upon a risk management framework that takes into account threats, vulnerabilities, and consequences when prioritizing CI/KR protection activities. It provides an integrated, comprehensive approach to addressing physical, cyber, and human threats and vulnerabilities to address the full range of risks to the Nation.

The Interim NIPP is the Base Plan that provides the framework and sets the direction for implementing this coordinated, national effort. It provides a roadmap for identifying CI/KR assets, assessing vulnerabilities, prioritizing assets, and implementing protection measures in each infrastructure sector. For each sector, the NIPP will delineate roles and responsibilities among Federal, State, local, tribal, and

## About the Interim NIPP

- **Why is this version “interim?”** This document provides the starting point for developing the national, cross-sector plan for critical infrastructure protection.

*The national and sector-specific programs that will be implemented under this Interim Plan vary widely in development and progress—some have been successfully operating for years, while others were more recently established. The Interim NIPP builds on the existing base, while acknowledging the need to expand dialogue and partnerships with the private sector and other stakeholders to create an integrated, national CIP program.*

- **What does the Interim Plan do?** This first iteration of the Plan takes the principles of the National Strategy for Homeland Security (DHS, July 2002) to the next level to ensure consistent and comprehensive identification of assets, assessment of vulnerabilities, and prioritization of assets to guide the effective implementation of protective programs.

*This Base Plan identifies the general roles and responsibilities for each set of stakeholders, highlights best practices and initiatives already underway, and introduces features, such as metrics and stakeholder engagement, for ensuring that the program is successful. It also addresses the need for identifying market-based incentives and other mechanisms to encourage voluntary implementation as well as protecting sensitive business information.*

- **What does the Interim Plan NOT do?** It does not substitute for the ongoing partnerships among DHS, the Sector-Specific Agencies, other Federal departments and agencies, the private sector, and State, local, and tribal entities.

*This Interim Plan is the starting point for building the national program and for initiating extensive dialogue with State, local, and tribal entities as well as private sector stakeholders to obtain their perspectives on protecting critical infrastructure.*

- **What’s next?** DHS, the Sector-Specific Agencies, and other Federal departments and agencies will work with the private sector and State, local, and tribal entities to further refine stakeholder roles and responsibilities and implement the NIPP (Base Plan) and the Sector-Specific Plans (SSPs) that will become annexes to the NIPP.

*The specific steps will be delineated in an implementation strategy developed by DHS. The results of these implementation efforts will be reflected in the next version of the NIPP, which will be issued within 270 days of issuance of this interim document.*

private sector stakeholders in carrying out these activities, with DHS as the lead agency and single point of accountability and coordination.

## 1.2 Organization and Scope

In addition to this introduction, the Interim NIPP consists of the following chapters:

- Chapter 2—National Goals, Framework, and Actions
- Chapter 3—Vulnerability Reduction Program
- Chapter 4—Threat-Initiated Actions
- Chapter 5—Roles and Responsibilities
- Chapter 6—Integration with Other Plans

The scope and framework of the Interim NIPP are established in Homeland Security Presidential Directive-7 (HSPD-7), “Critical Infrastructure Identification, Prioritization, and Protection,” issued in December 2003. HSPD-7 identifies 17 specific CI/KR sectors. Consistent with HSPD-7, the NIPP addresses on-going as well as future activities to be carried out both within these 17 individual CI/KR sectors and

nationally across sectors. The Interim NIPP describes DHS leadership of the effort to integrate CI/KR protection activities across sectors.

The Interim NIPP focuses on protection of our Nation’s most critical assets within our borders as well as addressing any international linkages. For cyber infrastructures, the United States will work with foreign governments and international organizations to enhance the reliability, availability, and integrity of the Internet. For physical assets located on or near borders with Canada or Mexico, the consequences of an attack may affect the bordering country; protection of the particular asset may require the coordination with or resources from the bordering country. Protection is also necessary when a sector’s infrastructure is extensively integrated into an international or global market (e.g., financial services) or when the proper functioning of a sector relies on inputs that are not within our Nation’s control. In particular, tampering with or disrupting the flow of critical raw materials into the United States (e.g., by contaminating agricultural products or obstructing transport of energy sources or industrial raw materials), may cause cascading failures within the sector. Therefore, the Interim NIPP includes consideration of these international

interdependencies and the vulnerability of assets to threats that originate outside the country.

### 1.3 Definitions

This section defines key terms used in the Interim NIPP. The term “critical infrastructure” is defined as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”<sup>1</sup> “Key resources” are “publicly or privately controlled resources essential to the minimal operations of the economy and government.”<sup>2</sup> “Key assets” (a subset of key resources) are “individual targets whose destruction could cause large-scale injury, death, or destruction of property, and/or profoundly damage our national prestige and confidence.”<sup>3</sup>

Critical infrastructure and key resources are composed of one or more assets. In this document, an asset is something of importance or value and can include one or more of the following types of elements:

- **Human**—The human aspect of an asset includes both the employees to be protected and the personnel who may present an insider threat (e.g., due to privileged access to control systems, operations, and sensitive areas and information).
- **Physical**—The physical aspect may include both tangible property (e.g., facilities, components, real estate, animals, and products) and the intangible (e.g., information).
- **Cyber**—Cyber components include the information hardware, software, data, and networks that serve the functioning and operation of the asset.

The term “sector-specific” agency refers to those Federal departments and agencies identified under HSPD-7 as responsible for the protection activities in specified CI/KR sectors. Exhibit 1 identifies the SSAs and the specific sectors for which they are responsible<sup>4</sup>, in coordination with supporting agencies.

The terms “protect and secure,” as defined in HSPD-7, mean

#### Exhibit 1: Sector-Specific Agencies and Assigned Sectors

**Department of Agriculture** — Agriculture, food (meat, poultry, egg products)

**Department of Health and Human Services** — Public health and healthcare; Food (other than meat, poultry, egg products)

**Environmental Protection Agency** — Drinking water and wastewater treatment systems

**Department of Energy** — Energy, including the production, refining, storage, and distribution of oil and gas, and electric power (except for commercial nuclear power facilities)

**Department of the Treasury** — Banking and finance

**Department of the Interior** — National monuments and icons

**Department of Defense** — Defense industrial base

**Department of Homeland Security**<sup>5</sup> —

- Information technology
- Telecommunications
- Chemical
- Transportation systems<sup>6</sup>
- Emergency services
- Postal and shipping
- Dams
- Government facilities
- Commercial facilities
- Nuclear reactors, materials, and waste<sup>7</sup>

reducing the vulnerability of CI/KR in order to deter, mitigate, or neutralize terrorist attacks. Thus, as described in this Interim NIPP, critical infrastructure protection includes the activities that identify CI/KR, assess vulnerabilities, prioritize CI/KR, and develop protective programs and measures, because these activities ultimately lead to the implementation of protective strategies to reduce vulnerability.

<sup>1</sup> See USA PATRIOT Act of 2001, 42 U.S.C. § 5195c(e), defining critical infrastructure. This definition is incorporated by reference into the Homeland Security Act of 2002, see 6 U.S.C. § 101.

<sup>2</sup> Homeland Security Act, Section 2(9).

<sup>3</sup> National Strategy for the Physical Protection of Critical Infrastructures and Key Assets” (February 2003), page 7.

<sup>4</sup> Paragraph 18 of HSPD-7 except for Department of Homeland Security.

<sup>5</sup> Paragraph 15 of HSPD-7.

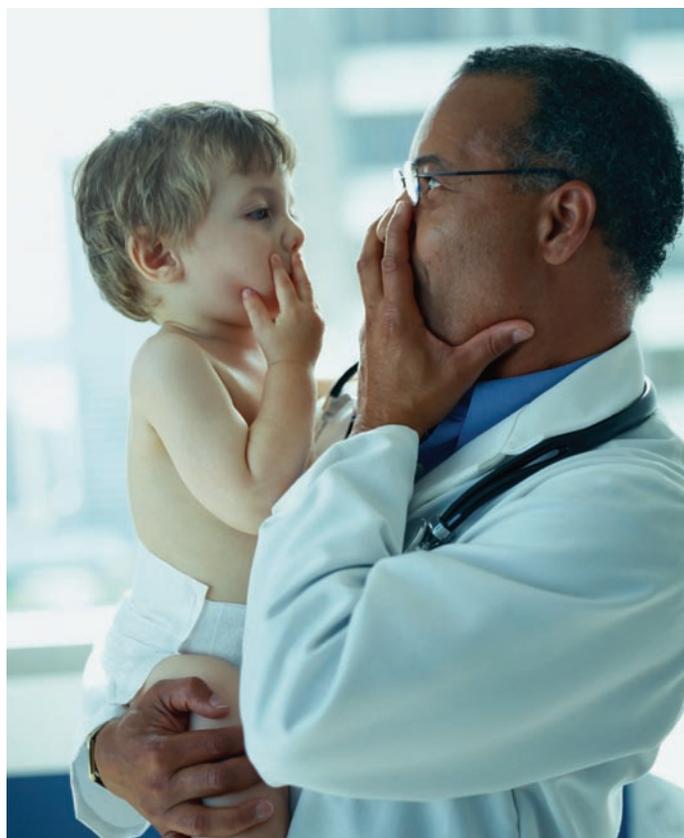
<sup>6</sup> Per Section 22(h) of HSPD-7, DHS and the Department of Transportation will collaborate on all matters relating to transportation security and transportation infrastructure protection.

<sup>7</sup> Under Paragraph 29 of HSPD-7, DHS will work with the Nuclear Regulatory Commission and, as appropriate, DOE in order to ensure the necessary protection of commercial nuclear reactors, research and test nuclear reactors, nuclear materials, and the transportation, storage, and disposal of nuclear materials and waste.

## 1.4 Key Stakeholders and Partnerships

Although DHS is ultimately accountable for the success of the Nation's CIP program, implementation requires an integrated process across all of the key infrastructure protection stakeholders. These stakeholders include:

- **Department of Homeland Security**—The Department of Homeland Security is the lead agency for the overall national effort to enhance CI/KR protection. In this role, DHS establishes uniform policies and approaches for protection activities, and tracks performance and progress in program implementation. DHS is also the lead agency for the overall assessment of the terrorist threat to the Nation. Building on the efforts of the SSAs, DHS maintains the national inventory of CI/KR assets and carries out national and cross-sector vulnerability assessments, asset prioritization, and, where appropriate, protective measure implementation. DHS also provides specific expertise in addressing the physical, human, and cyber elements of CI/KR, and serves as the lead agency for coordination and information sharing among sector stakeholders.
- **Sector-Specific Agencies**—The SSAs provide the subject matter and industry-specific expertise and relationships to ensure infrastructure protection within the specific sec-



tors. Each SSA is responsible for developing, implementing, and maintaining a Sector-Specific Plan for conducting CIP activities within the sector, which include collaborating with all relevant Federal departments and agencies, State and local governments, and the private sector; identifying assets; conducting or facilitating vulnerability assessments; and encouraging risk management strategies to protect against and mitigate the effects of attacks against CI/KR. While DHS is the SSA for multiple sectors, some organizational elements within DHS have been designated to have primary sector-specific responsibility and are included when referring to SSAs. For example, the Transportation Security Administration (TSA) has this responsibility for the transportation systems sector and the National Cyber Security Division has this responsibility for the information technology sector. The purpose of this designation is to ensure that one organizational element within DHS is the single point of contact and has ultimate accountability for developing the SSP and implementing related CIP activities.

- **Other Federal Agencies**—Federal departments and agencies not designated as SSAs may, nevertheless, provide critical support in the protection of a given sector. Specifically, Federal departments and agencies may provide information on aspects or parts of the sector, or may play a role as the regulatory agency for many owners and operators represented in the sector. Some agencies (e.g., Department of State) may support international outreach to foreign countries or international organizations to strengthen protection of CI/KR.
- **Private Sector**—Because private industry owns and operates the vast majority of the Nation's CI/KR, its involvement is crucial for successful implementation of the NIPP and the national CIP program. Private-sector owners and operators remain the first line of defense for their own facilities and routinely carry out risk management planning and invest in protective measures as a necessary business function. Through various means, the private sector obtains and shares security-related information with Federal, State, and local agencies. As the NIPP is developed and implemented, the specific role of the private sector in the national CIP program (including within each sector) will continue to evolve and be further defined and enhanced.
- **State, Local, and Tribal Entities**—State, local, and tribal entities constitute the front line of response and defense in support of the security spectrum, and may also act as conduits for requests for Federal assistance when the threat exceeds their capabilities. For certain CI/KR, State, local, and tribal entities may serve as owners or

operators of a significant portion of their infrastructure. Furthermore, the Homeland Security Advisor (HSA) in each State serves as the principal point of contact for DHS on homeland security issues. Similar to the private sector, the specific role of State, local, and tribal entities in national CIP will continue to be refined and enhanced as the Interim NIPP is implemented.

In order for the national critical infrastructure protection program to be successful, there must be efficient and effective partnership, communication, and coordination among DHS, SSAs, other Federal departments and agencies, private sector owners and operators, and State, local, and tribal entities. The means of partnering with sector stakeholders is evolving as each sector becomes better defined. Prior to the creation of DHS, an architecture of Sector Coordinators and Information Sharing and Analysis Centers (ISACs) was created that began this partnership and achieved early successes. With the creation of DHS and the development of the NIPP, this partnership must evolve to meet new requirements for enhanced capabilities and a revised framework. The NIPP envisions the following three components to implement the public-private partnership:

- **The NIPP Senior Leadership Council**—Will be comprised of the leadership of the Federal departments and agencies engaged in critical infrastructure protection with critical infrastructure owners and operators and State Homeland Security Advisors (HSAs) to lead, integrate, and coordinate the implementation and continuous enhancement of the NIPP through the following activities: advancing collaboration and information sharing within and across sectors, forging consensus on critical infrastructure protection action, evaluating and promoting implementation of risk management-based infrastructure protection programs, and evaluating and reporting on progress. The NIPP Senior Leadership Council is supported by the Cross-Government Coordinating Council and the Cross-Sector Coordinating Council.
- **CI/KR Sector Coordinating Councils**—Are private sector coordinating mechanisms that comprise private sector infrastructure owners and operators and supporting associations, as appropriate. Sector Coordinating Councils bring together the entire range of infrastructure protection activities and issues to a single entity. One role of the Sector Coordinating Councils is to identify or establish and support the information sharing mechanisms (ISMs) that are most effective for their sector, drawing on existing mechanisms (e.g., ISACs) or creating new ones as required.



- **CI/KR Government Coordinating Councils**—Are Government Coordinating Councils for each sector comprised of representatives from DHS, the SSA, and the appropriate supporting Federal departments and agencies. The Government Coordinating Councils work with and support the efforts of the Sector Coordinating Councils to plan, implement and execute sufficient and necessary broad-based sector security, planning and information sharing to support the Nation's homeland security mission.

Chapter 5 of this Interim Plan provides more detailed information on the specific roles and responsibilities of these stakeholders and coordinating mechanisms.

## 1.5 Next Steps

The national CIP program will be an ongoing effort to protect the Nation's CI/KR. As one of the initial steps in this program, DHS and the SSAs will share and discuss the NIPP framework with the different stakeholders described above to obtain and consider their feedback. Simultaneously, SSAs will work with their stakeholders to begin implementation of the SSPs, so that protective programs and limited resources are targeted at the most critical assets within and across sectors. Success will be achieved by working together through public and private sector partnerships to identify, prioritize, and protect the Nation's CI/KR. Key next steps for different stakeholders include:

- **Private Sector**—The private sector will be engaged by DHS, in collaboration with the relevant SSAs, to promote awareness of and feedback on the NIPP framework and to solicit their involvement in the national CIP program. The private sector will also be working with the appropriate SSAs to begin implementation of the SSPs for their sectors.

As the Interim NIPP is implemented, the private sector should expect more coordinated data calls from government agencies, enhanced engagement through Sector Coordinating Councils, and subsequent versions of the NIPP and SSPs will reflect discussions among DHS, the SSAs, and other stakeholders, including the private sector.

- **State, Local, and Tribal Entities**—State, local, and tribal entities will also be engaged by DHS and the SSAs to promote awareness of and provide feedback on the NIPP framework and to solicit their involvement in the national CIP program. The State, local, and tribal entities will also work with the appropriate SSAs to begin implementation of the SSPs for various sectors. As the NIPP is implemented, State, local, and tribal government agencies should expect to experience more coordinated data calls, fewer overlapping efforts to identify and assess critical assets, and subsequent versions of the NIPP and SSPs will reflect discussions between the DHS, the SSAs, and other stakeholders, including State, local, and tribal government agencies.
- **Sector-Specific Agencies**—The SSAs will be key participants in the DHS outreach strategy and have their own dialogue with State, local and tribal entities and the private sector. The SSAs will begin implementing the SSPs, making progress on the initiatives outlined in the SSPs and working with all their respective stakeholders so that SSPs meet the unique challenges of each individual sector.



SSAs will utilize, refine, and continue to develop milestones and performance measures to assess progress in each sector. Cross-sector coordination will occur through the NIPP Senior Leadership Council and specific parts of DHS that will be conducting interdependency analyses, developing guidance and tools, and working on a measurement system that provides important feedback to the SSAs.

- **Other Federal Agencies**—Supporting departments and agencies will work with the SSAs to implement the SSPs and participate in sector-specific activities through the Government Coordinating Councils.
- **Department of Homeland Security**—DHS/Information Analysis and Infrastructure Protection (IAIP) Directorate will undertake a major outreach effort to engage all the stakeholders necessary to make the national CIP program a success. In doing so, DHS will work with stakeholders to utilize, refine, and continue to develop milestones and performance measures to assess national-level and sector-by-sector progress. At the same time, it will continue to enhance its programs in information analysis and infrastructure protection and integrate these efforts under the framework of the NIPP.

# 2. National Goals, Framework, and Actions

This chapter outlines the national goals and objectives of the NIPP, including the legislative and policy drivers behind those goals, introduces the risk-management framework that supports the national goals, and presents key actions that are crucial to meeting overall goals.

## 2.1 Goals and Objectives

The national CIP effort is an evolutionary process. The need for infrastructure protection was reiterated in the Homeland Security Act of 2002, which established the IAIP Directorate. The vision for the Nation's CIP program was initially communicated through the July 2002 "National Strategy for Homeland Security." In February 2003, the President issued more specific strategies for physical protection of CI/KR, and for the protection of cyberspace.<sup>8</sup> The DHS Strategic Plan (February 2004) further emphasized the need for infrastructure protection.

Although the Homeland Security Act and subsequent strategies collectively defined what must be done to protect the CI/KR, they did not define how this would be accomplished. Although some strategies tailored for specific infrastructures have existed for several years, they do not

constitute an overall national CIP program. In December 2003, the President issued HSPD-7 to direct the activities of the CIP effort.<sup>9</sup> HSPD-7 provides this guidance by directing Federal departments and agencies to identify, prioritize, and coordinate the protection of CI/KR. It also requires that DHS take a leadership role with other Federal departments and agencies in working with State, local, and tribal entities and the private sector to carry out these responsibilities. HSPD-7 also identified the NIPP as the mechanism for consolidating and documenting national CIP activities.

Building on the foundation created by these efforts, the five overarching goals of the Interim NIPP are outlined in exhibit 2. The objectives below each goal indicate the desired result.

### Exhibit 2: Interim NIPP Goals and Objectives

#### Goal 1: Protect CI/KR against plausible and specific threats

##### *Objectives to meet goal include:*

- Increase awareness of the threat environment across CI/KR sectors
- Integrate threat and vulnerability information into specific vulnerability reduction prioritization decisions
- Use vulnerability assessment information when responding to specific threats
- Identify and implement protective measures against specific threats

#### Goal 2: Long-term reduction of CI/KR vulnerabilities in a comprehensive and integrated manner

##### *Objectives to meet goal include:*

- Develop and maintain comprehensive national inventory of CI/KR assets and vulnerabilities that includes cyber, physical, and human aspects of each asset, including intangibles
- Complete mapping of interdependencies among assets and across CI/KR sectors
- Conduct vulnerability assessments for the Nation's critical infrastructure and key resources for both specific and general threats
- Integrate infrastructure protection activities with those called for in other national-level plans to avoid overlaps and gaps
- Reduce general vulnerabilities within and across sectors where needed

<sup>8</sup> "The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets" and "The National Strategy to Secure Cyberspace" (February 2003).

<sup>9</sup> Homeland Security Presidential Directive 7 (HSPD-7)—"Identifying, Prioritizing, and Protecting Critical Infrastructure" (December 17, 2003). HSPD-7 replaces Presidential Decision Directive (PDD) 63—"Critical Infrastructure Protection" (May 1998).

## Exhibit 2: Interim NIPP Goals and Objectives (*continued*)

### Goal 3: Maximize efficient use of resources for infrastructure protection

#### *Objectives to meet goal include:*

- Prioritize possible protective measures considering return-on-investment in light of inherent vulnerabilities, existing protective measures, and (when applicable) threat information
- Encourage and support SSA responsibility for sectors to leverage sector-specific expertise
- Identify market-based incentives for voluntary action by owners and operators
- Ensure lessons learned and best practices are captured and shared for evolution into sector-accepted operational practices over time

### Goal 4: Build partnerships among Federal, State, local, tribal, international, and private sector stakeholders to implement CIP programs

#### *Objectives to meet goal include:*

- Delineate roles, responsibilities, and accountability for actions
- Develop necessary organizations, staffing, and training to carry out responsibilities
- Request appropriate authorities and funding to allow actions to be implemented
- Establish mechanisms for coordination and information exchange among partners
- Develop mechanisms for tracking involvement and progress

### Goal 5: Continuously track and improve national protection

#### *Objectives to meet goal include:*

- Develop mechanisms for tracking national- and sector-level vulnerabilities and progress in reducing those vulnerabilities
- Make infrastructure protection activities and metrics part of the organization's overall operational metrics to reinforce the importance of CIP initiatives and activities
- Develop a national risk profile (a high-level summary of the risk and protection for all sectors) to align threats with strategic decision making
- Develop an information sharing system to support rapid dissemination of lessons learned

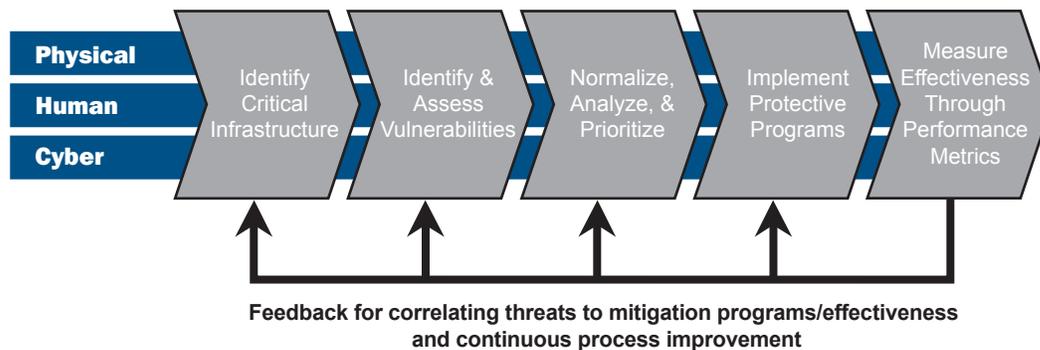
## 2.2 NIPP Risk Management Framework

To meet these national goals and objectives, the Interim NIPP utilizes a risk management framework that ensures that risk-reduction and protection measures are applied where they offer the most benefit. Under such a framework, risks can be managed in response to:

- **Specific threats**—situations where there is intelligence regarding targeted locations, sectors, or assets or when activity by groups known to favor certain types of assets is suspected. The likelihood of the threat is of particular concern in such situations, and will drive short-term protective measures.
- **General threat environment**—situations where the range of actions/threats that may plausibly occur within

a particular sector and to a particular asset is known, but there is no specific information regarding whether such an event appears to be in development. Plausible threats are those threats that could logically occur and that would have negative consequences on a particular asset. In this context, the plausible threats are treated as equally likely to occur to ensure that long-term protective programs are sufficiently inclusive of the range of threats. Thus, the protective response focuses on the inherent vulnerabilities of different assets and the potential consequences if the assets were attacked, rather than the likelihood of a particular event. For example, within the dams sector, the focus would be on the consequence of failure of a particular dam, and the protective actions that would reduce the vulnerability of failure. It would be assumed that any of the events that could result in dam failure would

### Exhibit 3: CIP Risk Management Framework



be equally likely to happen, because there would be no specific information regarding likelihood of one event over another. As a result, the best protective programs for different situations are determined using available threat information and intelligence, whether specific or general. Thus, the strategy is to be risk managed, but threat driven.

#### 2.2.1 Five-Step Process

The national CIP program is based on a risk management framework, continuously influenced by an ever-changing threat environment, with the goal of reducing the vulnerability of our Nation's assets to terrorist attack. As shown in exhibit 3, this framework involves five key steps, which are carried out both within sectors and nationally across sectors to protect CI/KR. These steps are part of an ongoing process, with the steps carried out as needed to narrow down the overall set of assets to those most critical at a national level. The basic elements of these steps are described below, and greater details are provided in the subsequent chapters of this Interim NIPP. The specific processes will be further refined and developed as the NIPP is implemented.

1. **Identifying critical assets**—The first step is identification of CI/KR assets across the 17 sectors. This identification is an ongoing process carried out by both the SSAs and DHS. The information collected is used as the basis for further decisions, which may include conducting vulnerability assessments and taking immediate protective actions depending on the threat environment and the need.
2. **Identifying and assessing vulnerabilities**—Vulnerability assessments are conducted for critical assets to identify both potential areas of weakness (against plausible threats) and those protective measures that would be effective to mitigate the weaknesses. A key challenge in assessing vulnerabilities is understanding the interdependencies among assets and sectors, so that cascading

impacts can be minimized. Vulnerability assessments also take into account international elements that may have a cascading effect on national CI/KR.

3. **Normalizing, analyzing, and prioritizing study results**—DHS and the SSAs must align the results of the many distinct assessment methodologies currently being used to assess vulnerabilities by first normalizing the information in a particular sector, and then prioritizing across the broader set of assets from multiple sectors. This process identifies the sectors, subsectors, regions, or specific assets that pose the greatest risk, and therefore offer the greatest benefit if protective actions are taken.
4. **Implementing protective programs**—Using information developed in the steps above, decisions are made regarding development and implementation of protective programs to reduce risk for the highest priority assets from both specific threats and general areas of vulnerability. To ensure that protective actions are implemented, DHS will work with various Federal departments and agencies and consult with the private sector to identify cost-effective incentives or strategies for enhanced security investments. DHS will work closely with other Federal agencies, State, local, and tribal entities to assist as needed in the allocation of limited resources, and will also work with the Department of State to conduct international outreach through bilateral and multilateral forums to address international vulnerabilities that affect the United States.
5. **Measuring performance**—To ensure that protective programs are applied consistently and are sustainable and effective, performance metrics are used to monitor the outcomes of the process for identifying critical assets, conducting vulnerability assessments, and applying protective programs. These measurements drive continuous process improvement across the risk management framework by highlighting framework steps that can be

modified or improved to drive more effective risk reduction and protective program implementation.

These activities are executed in an integrated manner across sectors, and address the physical, human, and cyber elements of the CI/KR. Many critical infrastructures also cross international borders, requiring further coordination of protection efforts.

### 2.2.2 Two-Pronged Implementation

The five steps described above take place in the context of an ever-changing threat environment. As discussed above, protective measures are undertaken both in response to specific threat intelligence and under the more general threat environment. Thus, as discussed in this Interim NIPP, the risk management framework is carried out in two ways:

1. **Vulnerability reduction program**—The five steps are carried out under the general threat environment (e.g., in the absence of specific threat information) to reduce CI/KR vulnerabilities in general and improve overall preparedness. In this process, the likelihood of plausible threats is considered equal.
2. **Threat-initiated actions**—In the context of specific threat information, DHS reviews existing information on CI/KR, their vulnerabilities, and established protective action programs. Based on this analysis, DHS, in consultation with relevant SSAs, issues threat warnings and recommends or undertakes certain protective actions.

The benefits of the framework are listed in exhibit 4.

Chapters 3 and 4 describe the activities carried out under each approach. This two-pronged approach not only ensures that known threats are addressed as needed, but also allows

#### Exhibit 4: Benefits of Risk Management Framework

- Implements a systematic, integrated approach that addresses the physical, human, and cyber elements of CI/KR assets within and across sectors
- Addresses threats and vulnerabilities, including interdependencies
- Provides a common framework within which risks are assessed, managed, and mitigated and progress is measured
- Creates a single, familiar common language for protection activities across both public and private stakeholders
- Offers flexibility and adaptability as threats, vulnerabilities, and potential consequences evolve
- Integrates key protection and analysis elements
- Enables DHS, other Federal departments and agencies, State, local, and tribal entities, and private sector owners to develop budgets and plans for effective resource allocation, including both protective programs and R&D efforts, that are matched to the prioritization of risks

the more systematic or planned implementation of protective programs to ensure preparedness for unknown future threats in each sector. Defining the roles of different parties for each prong also helps to ensure that resources are applied effectively and that there is minimal overlap in efforts.

### 2.3 Core Actions

The development of the NIPP, including the SSPs, will be a dynamic, iterative process that allows for and encourages continuous learning and improvement. Even though chapters 3 and 4 describe implementation actions, there will be variations in the manner by which individual SSAs implement their SSPs, depending on the nature and criticality of the assets within their sectors. Nevertheless, there are core activities that DHS and other stakeholders, including SSAs and other Federal agencies; the private sector; and State, local, and tribal entities will be expected to carry out to support the national goals and objectives. Strong partnerships across all of these groups are necessary to meet these expectations. Arranged by the goals they support, these core activities include:

#### Goal 1: Protect CI/KR Against Plausible and Specific Threats

- Develop and implement sector-specific and cross-sector



protective actions

- Conduct cross-sector interdependency analysis based on sector-specific data
- Protect sensitive and critical infrastructure related information from unauthorized disclosure

### **Goal 2: Long-term Reduction of CI/KR Vulnerabilities in a Comprehensive and Integrated Manner**

- Identify CI/KR assets and regularly update information
- Conduct and update vulnerability assessments at cross-sector, sector, and asset levels
- Analyze and store vulnerability assessment data and share with other key parties within legal constraints
- Develop and deploy new technologies to protect CI/KR

### **Goal 3: Maximize Efficient Use of Resources for Infrastructure Protection**

- Develop, maintain, and disseminate self-assessment tools
- Normalize and prioritize assets within and across sectors
- Draw on expertise across organizational boundaries
- Share lessons learned to minimize redundant efforts

### **Goal 4: Build Partnerships among Federal, State, Local, Tribal, International, and Private Sector Stakeholders to Implement CIP Programs**

- Establish and maintain SSA organizational structures for implementing CIP programs
- Develop and maintain partnerships with stakeholders
- Develop partnerships within DHS and across SSAs

- Develop partnerships between the international community and/or DHS and SSAs as appropriate
- Expand sector participation in information sharing
- Share information across all boundaries in a timely manner

### **Goal 5: Continuously Track and Improve National Protection**

- Establish performance metrics with which to measure the efficacy of protective measures
- Track and communicate CI/KR protection performance
- Update NIPP (and SSPs) as needed
- Ensure that initiatives support goals and objectives



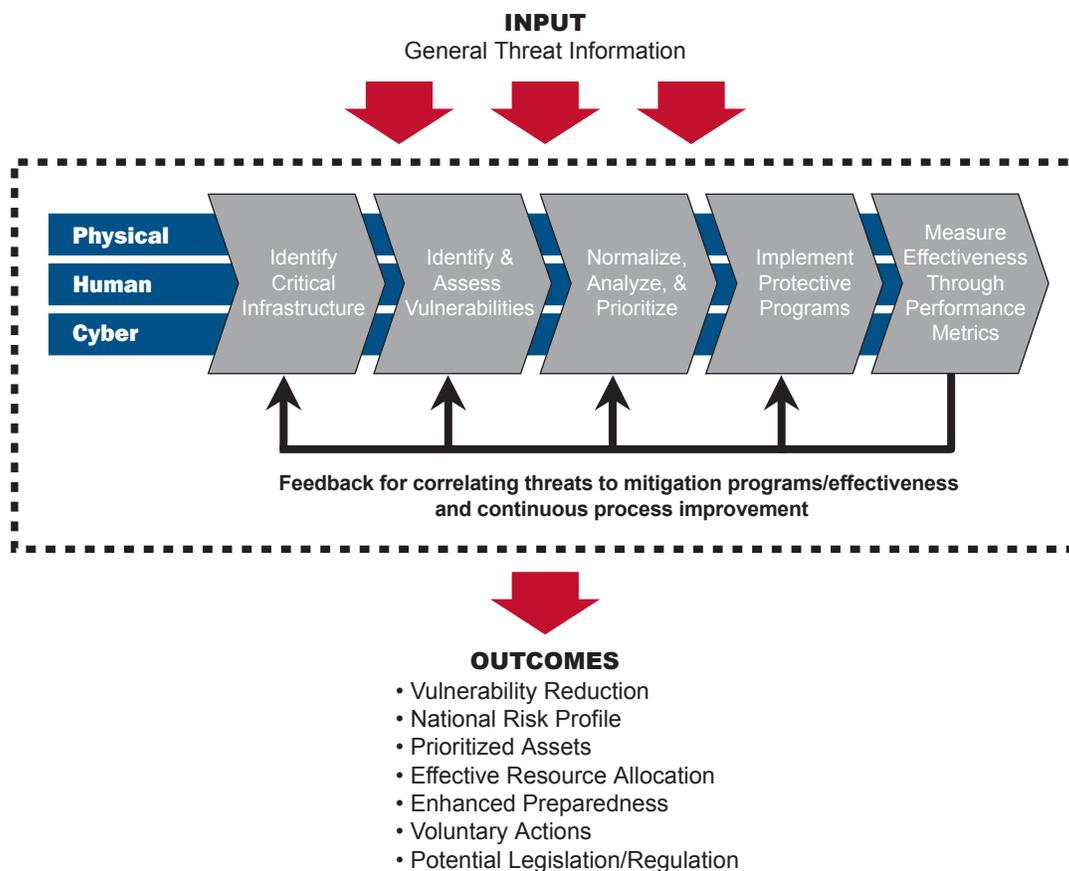
# 3. Vulnerability Reduction Program

As discussed in the previous chapter, the national CIP program is implemented both in response to specific threat information and in the more general environment of the range of plausible threats. This chapter of the Interim NIPP presents the concept of operation for the vulnerability reduction program that DHS, SSAs, and other stakeholders carry out to protect CI/KR in the general threat environment to improve overall protection capacity. In this context, the stakeholders work together to identify CI/KR, identify and assess vulnerabilities, prioritize CI/KR, and establish protective action programs based on general threat information for each sector. As the NIPP is implemented, the specific activities and responsibilities presented below will be further refined and developed.

Exhibit 5 illustrates the risk-management framework as applied to the vulnerability reduction program. As shown in the exhibit, general threat information sets the context for subsequent evaluations but does not drive specific analyses. The processes of asset identification and vulnerability

assessment consider the general threats to different types of assets in order to identify high-priority or high-value assets requiring protective programs, but these processes are not driven by specific threats. As noted in chapter 2, this process is ongoing and repeated as needed to reflect major changes

**Exhibit 5: Vulnerability Reduction Program**



in the threat environment or significant changes in assets, their vulnerabilities, and/or their protective programs.

The overall outcome of the vulnerability reduction program is an enhanced state of asset protection and vulnerability reduction through the implementation of focused protective strategies across the CI/KR sectors. The specific outcomes of the vulnerability reduction program are as follows:

- The national risk profile, which will be developed by DHS on an ongoing basis, is a high-level “snapshot” summary of the risk and protection for all sectors and can be used as the basis for strategic decision making, particularly with regard to Federal resource allocation and potential regulations or policy development. This profile will constantly change as protective programs are implemented for more assets.
- By developing a comprehensive national picture of CI/KR and their vulnerabilities, DHS and the SSAs, along with their governmental stakeholders, can prioritize assets within and across sectors to ensure that subsequent efforts and resources are placed where they offer the greatest overall benefit.
- This prioritized information will then be used to identify specific protective programs for the most critical (high-risk or high-value) assets, along with a schedule for their implementation so that resource allocation can be planned. Depending on the protective program, resource allocation may occur at the Federal, State, and/or local level, or may be allocated solely from the owners and operators. International outreach may also be required in certain circumstances.
- Depending on the findings of the analyses, the SSA or DHS will determine the best and most successful course of action to reduce vulnerabilities and enhance security. The possible range of available options, depending in part on the existing statutory authorities, includes: encouraging voluntary implementation (e.g., through public-private partnerships); pursuing incentive-related policies and programs; or seeking regulatory options.

The majority of the SSAs’ efforts will support the ongoing vulnerability reduction program, with DHS’s role in this area also growing over time as more information is available from each sector. DHS’s efforts will focus on cross-sector analysis (using the analyses provided by the individual sectors) to identify common vulnerabilities, establish and



implement protective measures to reduce vulnerabilities, and identify specific R&D needs. In addition, DHS will conduct evaluations of interdependencies and develop tools and guidance that can be used by the SSAs to improve their processes and analyses.

The application of each step of the risk management framework for vulnerability reduction is outlined below and will be supported by the detailed plans (SSPs) that the SSAs are preparing to describe their specific efforts for each part of the framework. The details of the approaches vary by sector. This is both expected and reasonable, given that different sectors have different characteristics and are at different stages of maturity and cohesion. Some sectors have proposed processes or the mechanisms for developing processes, while others were able to define the details of the specific processes to be applied. Some sectors already have results obtained from following existing processes, while others have results, but need to create processes, so that results can be obtained on an ongoing basis.

In addition, it is recognized that the assets themselves vary in criticality from one sector to another—some sectors have many critical assets while others have only a few. The number and type of asset classes in each sector range from a few (for relatively similar assets) to an extremely diverse set, each with its own stakeholders. The resources available to the SSAs are also quite variable, as are the relationships with and contributions of the private sector, and Federal, State, and local authorities, to the development of processes and tools and implementation of protective programs. The evolution of these relationships and development of vulnerability-reduction programs and processes will be reflected in future iterations of the NIPP.

The general threat environment will change as the capabilities and intentions of terrorists evolve. The Information Analysis (IA) Division of IAIP will assist the SSAs by routinely providing information about general threats to support the effective implementation of the risk management framework's steps. This will be facilitated by the SSA partnerships with the Infrastructure Protection (IP) Division of IAIP, and through their membership in the NIPP Senior Leadership Council (see Section 5.2.1 of this Plan).

### 3.1 Identify CI/KR

Infrastructure protection focuses on those CI/KR assets and events that, if attacked, could have the most catastrophic effect on the Nation. In making this determination, such factors as lives lost, economic impact, and national security impact are considered. As infrastructures are built or taken out of service, and technologies controlling these infrastructures change, there is a need to keep track of the universe of infrastructure assets that are critical to the Nation's functioning. Therefore, the first step in the framework is developing and maintaining an active and constantly updated inventory of CI/KR assets within and across sectors, including not only physical assets, but also the human and cyber components of various infrastructure systems. Furthermore, this includes not only assets within the United States, but also those on international borders or those affected by international concerns.

Sector-specific agencies are systematically collecting and updating data on assets within their sectors. In addition, DHS has a database of CI/KR assets that is used as a tool for making decisions at the national level regarding the need for protective actions. Under a risk management framework (described below), this asset information is combined with vulnerability assessment information to serve as the basis for further analyses within and across sectors to select assets warranting additional protective actions. Both DHS and SSAs will be working with the private sector to determine the most effective means of obtaining and analyzing this information. Furthermore, DHS is developing programs to ensure that access to and use of all these data are carefully controlled to protect the security of individual assets, the sectors, and the Nation, as well as to protect business confidential data. Exhibit 6 describes how DHS will protect voluntarily submitted data under the Protected Critical Infrastructure Information (PCII) program.

#### Exhibit 6: Protection of Critical Infrastructure Information

The Critical Infrastructure Information Act of 2002 (CII Act) called for the establishment of the Protected Critical Infrastructure Information (PCII) Program. To implement and manage the PCII Program, DHS created the PCII Program Office within the IAIP Directorate.

- Under the PCII Program, the private sector can voluntarily submit to the PCII Program Office sensitive and proprietary information about its critical infrastructure, with the assurance that the information, if it satisfies the requirements of the CII Act, will be protected from public disclosure to the maximum extent permitted by law.
- The PCII Program Office evaluates submitted critical infrastructure information to determine whether the requirements of the CII Act have been met and to validate the information as PCII.

#### 3.1.1 Sector-Specific Inventories

While CI/KR are predominantly owned and operated by the private sector, each SSA is responsible for identifying and maintaining current data on the CI/KR in its sector. The methodologies or processes that SSAs currently use or plan to use to collect such data from the asset owners and operators, and other data sources, will be described in Part II of each SSP. The resulting information (whether kept in a specific database or not) will be used by the SSA to coordinate protective actions within the sector. The asset information will also be used by IAIP/IP to support focused analyses in light of specific threat information and to coordinate national protective programs.

In addition to providing some level of detail on processes for identifying assets and gathering data, the individual SSPs will describe the manner in which each SSA proposes to coordinate with IAIP/IP to draw on past data collection efforts. Many of the SSPs will also describe mechanisms for making the data collection efforts more manageable such as by using a prioritized approach for reaching out to different stakeholders, the use of existing databases, and/or the determination of certain classes of assets that do not warrant data collection. The specific mechanisms and processes described below will continually evolve as the NIPP is implemented.

**Basic Asset Data.** The information collected by SSAs may include asset name, location, owner, and function, as well as

other information that may affect vulnerability, such as:

- System components that are central to the mission and function
- Dependencies (on what the asset depends in order to function)
- Continuity, redundancy (including backups), and resiliency built into the asset
- Existing protective actions (e.g., fencing, biometrics, firewalls, procedures, etc.)

**Interdependencies.** SSAs will also work with the asset owners and operators to gather data related to the asset's interdependencies and interconnectivity. Many assets are dependent on multiple elements and systems to maintain functionality, both at the sector level and more locally. In some cases, a failure in one sector will have a significant impact on the ability of another sector to perform necessary functions. Therefore, each SSP will include an analysis of the interdependencies among sectors, both at the sector-level and local level, including those interdependencies that may be exploited by terrorists. In addition, the SSAs will identify international interdependencies (e.g., where the functioning of the sector relies on imports/inputs not within the Nation's control).

**Consequences.** In creating the inventory of assets, SSAs will examine the inherent characteristics of the asset or system and identify the worst-case consequences that would result if the asset were destroyed, disrupted, or exploited. As set forth in HSPD-7, the focus is on potential for situations that could:<sup>10</sup>

- Cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction
- Impair Federal departments' and agencies' abilities to perform essential missions or to ensure public health and safety
- Undermine State, local, and tribal government capacities to maintain order or deliver essential public services
- Damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services
- Have a negative impact on the economy through the cascading disruption of other critical infrastructure and key resources

- Undermine the public's morale and confidence in our national economic and political institutions

The potential consequences are scored using categories or ranges to group assets by type and scale of potential impacts. The assets with potential consequences in the highest ranges for one or more of the consequence types will be of greatest concern for subsequent analyses. The consequences of concern have been tailored to each sector or asset class and its potential impacts.

**Range of Assets.** Although obtaining data for larger assets is relatively easy, the challenge is

also to ensure that smaller or less visible critical assets are also identified. Many small assets play a little-known but vital role in the nation's economy—particularly when interdependencies are recognized. For example, a small manufacturer of pharmaceuticals or vaccines could be the sole U.S. manufacturer of that product; similarly, a small plant could be the primary producer of a component that is vital to the defense industrial base. The search for smaller assets makes the effort more time-consuming, but it is a crucial part of the process if the full set of potential consequences is to be considered.

IAIP/IP will continue to work with the SSAs to use their sector-specific expertise to identify these assets and to ensure their inclusion in the national inventory. Both DHS and SSAs, in turn, will be engaging with the private sector to further identify how asset-specific information can be obtained and protected. For example, SSAs can send letters to various industry associations requesting that their members provide a set of basic information on their facilities. The efforts of the SSAs to obtain information on assets throughout sectors will greatly simplify the asset-identification process for DHS.



<sup>10</sup> Paragraph (7), sections (a) through (f) of HSPD-7.

### 3.1.2 National CI/KR Inventory

Successful infrastructure protection requires robust baseline data on the assets within and across infrastructure sectors, segments, and regions, among others. Thus, while SSAs are responsible for identifying CI/KR assets and collecting data within their sectors, IAIP/IP maintains the National Asset Database (NADB), which is a comprehensive catalog of asset information (not a listing of prioritized assets), to ensure the integrity of the national CI/KR inventory. Access to such a database allows common vulnerabilities and interdependencies to be defined and assessed not only by location, but also within and across sectors.

IAIP/IP has developed and will continue to build the NADB using a variety of sources. The input data may come from different Federal, State, and local databases; specific studies; data-call efforts; and the sector-specific data collection activities. Some of the specific data collection efforts that contributed to the earliest entries in the NADB include:

- **Ongoing data calls**—On an as-needed basis, IAIP/IP has asked that certain sector stakeholders voluntarily provide detailed information on high-risk targets. For example, in Operation Liberty Shield, State and local officials provided lists of high-risk assets.
- **State and local annual submissions**—Data submitted annually to the DHS Office for Domestic Preparedness (ODP) on CI/KR in their jurisdictions.
- **Voluntary submittals from sector stakeholders**—Private sector owners and operators, State and local governments, and Federal departments and agencies can nominate assets and locations to be included in the database at any time.
- **Results of prior studies**—Different studies undertaken by trade associations, advocacy groups, and regulatory agencies include lists of CI/KR.
- **Ongoing reviews of particular locations where threats are focused**—These IAIP/IP-initiated efforts not only provide information on vulnerabilities and interdependencies,

but also identify CI/KR in terms of potential consequences.

Within the Federal Government, many departments and agencies have been using a methodology called Project Matrix to help identify and prioritize internal critical functions, services, and assets and to map existing interdependencies to other assets. The results of these efforts may also be included in the NADB.

### 3.1.3 Updating and Using the Inventories

Although the earlier data collection efforts resulted in information that varied in format and quality, each new data collection effort, either by IAIP/IP or through the SSAs, provides more comprehensive information on the CI/KR inventory. IAIP/IP will work with SSAs, the private sector, and State, local, and tribal stakeholders to develop specific processes and mechanisms for gathering the sector-specific asset data for entry in the NADB. Because much of this information will be sensitive from both an infrastructure protection perspective and in terms of business competitive content, DHS will focus on developing appropriate data control and access procedures.

After the raw data are entered into the NADB, IAIP/IP uses objective standards, as well as expert opinions, to refine the universe of assets to a subset for further analysis and action at the national level. IAIP/IP first relies on subject-matter experts within various sectors to identify assets of potential national-, regional-, or sector-level importance. The resulting smaller set of assets is then further analyzed to determine the potential consequences that may result if the asset were compromised. This analysis is based on the inherent characteristics of the asset or system and involves identifying the worst-case consequences if the asset were destroyed, disrupted, or exploited. The analysis also considers the potential additional consequences of dependencies, interdependencies, and other impacts on the value chain. Through this analysis, IAIP/IP identifies “high value/high risk” assets (i.e., those with very high potential consequences or high vulnerability).

Based on this relatively high-level consequence assessment, IAIP/IP further refines the assets into a series of different classified planning tools that may focus on:

- High-risk urban areas
- High-risk assets
- National security special events (NSSEs) and other high-value/high-risk (HV/HR) special event sites
- HV/HR soft targets





- HV/HR overseas assets and HV/HR events
- High-value assets

The results of these analyses are a series of classified reports and a list identifying specific assets that are viewed as possible targets warranting protective measures. The list is identified by DHS as the Protective Measures Target List (PMTL). All or part of the PMTL may be made available to selected owners and operators, law enforcement agencies, and other members of the protective community. It is also used as the basis for vulnerability identification and analysis.

### 3.2 Identify and Assess Vulnerabilities

The second major step in the risk-management process is to identify and analyze the vulnerabilities of certain CI/KR assets or key events/locations identified in the step above. While the programs and processes in the Interim NIPP are focused on enhancing CIP in light of terrorism/security challenges, they have a broad applicability to all hazards. Thus, as used here, vulnerability is defined as the characteristics of an asset's design, location, or operation/use that render it susceptible to damage, destruction, or incapacitation by terrorist or other intentional acts, mechanical failures, and natural hazards. For cyber-specific assets, as well as the human and cyber elements of an asset, vulnerabilities may also be present as flaws in security procedures; software; internal system controls; or the design and use of an information or communication system that may affect the integrity, confidentiality, accountability, and/or availability of data or services. Vulnerabilities include flaws that may be deliberately exploited to affect that asset/system or to allow further access to other assets/systems, as well as those that may lead to failure due to inadvertent human actions or natural disasters.

A vulnerability assessment is a systematic process to measure the susceptibility of a sector, segment, region, or

individual site to attack. Through a vulnerability assessment, areas of weakness and potential actions that would exploit those weaknesses are identified, and the effectiveness of additional security measures is assessed.

As described below, vulnerability assessments can be carried out both within specific sectors and across sectors, focusing on assets and sites in the national inventory. Owners and operators in some of the CI/KR sectors will also routinely perform self-assessments (e.g., to satisfy existing regulatory requirements).

Within the designated sectors, the SSAs are responsible for facilitating or conducting the necessary vulnerability assessments—whether the assessments are conducted at the sector or subsector level by the SSA or are self-assessments carried out by the asset owners and operators or others (e.g., a State agency). Each SSP will describe the methodology used to assess vulnerabilities of assets in that sector, and describe how the assessments are carried out (e.g., by whom, how often, etc.). Some SSAs have a tiered strategy using different assessment tools and approaches for different groups of assets, so that the assets of greatest concern receive the most detailed examination, and others use less resource-intensive approaches. SSAs have also been encouraged to involve relevant stakeholders in creating or refining the appropriate processes and tools. The processes and tools that result from this stakeholder engagement will be reflected in future iterations of the NIPP.

As set forth in the Interim NIPP, vulnerability assessments consist of the following activities:

- Obtaining information and assessments from IAI/IA and other partners in the intelligence and law enforcement community on general and sector-specific terrorist capabilities
- Selecting the assets or asset classes to be assessed using the results of the sector-specific asset identification process
- Determining appropriate vulnerability assessment strategy (e.g., self-assessments, State- or Federally-led assessments, expert reviews, or third-party assessments)
- Identifying appropriate assessment methodologies/tools for the particular type of asset
- Establishing the assessment team
- Identifying interdependencies and connections with other assets and sectors
- Identifying physical, human (e.g., procedural), and cyber vulnerabilities
- Analyzing benefits of existing protective programs

- Assessing residual gaps to determine importance of vulnerabilities
- Grouping vulnerabilities by potential protective strategies (e.g., by type of attack, etc.)

Under the vulnerability reduction program, the vulnerability assessments focus on the potential weaknesses that could result in the consequences of concern. Thus, these analyses are not threat-driven—rather, it is assumed that all plausible hazards have equal probability of occurrence. The purpose is to identify the sector assets that should be considered high priority based on potential consequences if the asset were destroyed or compromised, and the likelihood of a successful attack. The second factor is a measure of the susceptibility or vulnerability to an attack (i.e., whether the asset would fail if an attack were to occur). Thus, it considers intrinsic structural weaknesses, protective measures, and redundancies. For example, if a facility is already physically hardened, then its vulnerability to a physical attack (e.g., explosive device) may be lower than the vulnerability of a similar facility that has not been hardened. The actual likelihood of the attack or event itself is not taken into account (or is assumed to be equal for all events).

IAIP/IP will also conduct vulnerability assessments as part of the vulnerability reduction program to:

- More fully investigate interdependencies within and between sectors. A high-level, top-down review may be more effective at identifying and assessing large-scale interdependencies than a bottom-up, asset-specific review. IAIP/IP will also be able to establish a more diverse assessment team with experience across sectors. Advanced modeling, simulation techniques, and sector-specific vulnerability identification and risk assessment methodologies will be used to enable an understanding of infrastructure interconnection and interrelation.
- Serve as a basis for developing common vulnerability reports that can help to identify strategic needs for protective programs or R&D across sectors or subsectors
- Fill selected gaps when sectors or asset owners or operators have not yet completed assessments, and such studies are needed immediately
- Test new methodologies or streamlined approaches to vulnerability assessments before making them generally available to the SSAs and their stakeholders

In some sectors and segments, vulnerability assessments have never been performed or have been performed for only a small number of high-profile or high-value sites. To help close this gap, IAIP/IP will provide the following



assistance to SSAs, other Federal agencies, and other sector stakeholders (e.g., owners and operators) as this Interim Plan is implemented:

- Help to determine the criteria for vulnerability assessments, particularly for critical assets
- Provide vulnerability assessment tools to be used as part of the self-assessment process
- Provide the Characteristics and Common Vulnerabilities reports and Potential Indicators of Terrorist Activity reports for industrial sectors, and classes of activities and HV/HR event sites
- Provide references of generally accepted vulnerability assessment processes for major classes of activities and HV/HR event sites
- Help to oversee the development and sharing of industry-based standards and tools
- Suggest the frequency of assessments, particularly in light of new types of threats
- For some high-risk assets, conduct Site Assistance Visits and perform the actual vulnerability assessments of specific sites and infrastructures

IAIP/IP uses the results of the vulnerability assessments to develop reports on specific vulnerabilities by location, by type of attack, or by associated consequence. When IAIP/IP personnel conduct the vulnerability assessment, they will ensure that any general lessons learned are documented and provided to the involved individual sectors, as well as to law enforcement staff and the private sector, for application to the full set of assets (particularly those that do not have the direct involvement of IAIP/IP).

IAIP/IP's goal is to add select vulnerability assessment data into the NADB, where they can be analyzed with other risk information to set priorities for the implementation of protective programs. Currently, any IAIP/IP vulnerability assessment results are maintained separately from the NADB. As the sectors develop programs and determine the quantity of data on vulnerability assessments they maintain, IAIP/IP will refine its expectations for, and approach to, retaining vulnerability assessment results. These changes will be reflected in future iterations of the NIPP.

### 3.3 Analyze, Normalize, and Prioritize CI/KR

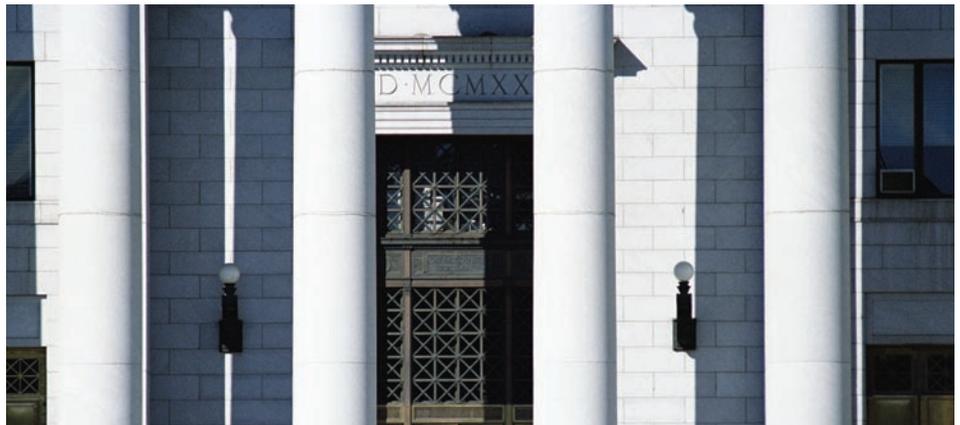
It is impossible to protect all of the infrastructure sectors equally across the entire United States. Because the vulnerabilities, threats, and potential consequences of an attack differ for individual assets and sectors, analysis is necessary to understand and prioritize risk across the infrastructure or various segments. In the absence of a specific threat, such analysis identifies the highest-risk assets that become the focus of longer-term resource decisions and protective programs.

#### 3.3.1 Analysis and Prioritization Process

The analysis and prioritization process consists of several steps: (1) normalization of data, to allow for analysis across sectors, including interdependencies; (2) risk analysis, in which vulnerabilities for high-consequence assets are compared against the general threat assessment; and (3) identification of priorities, based on overall reduction in risk relative to overall costs. This process will be carried out both within a sector (by SSAs) and at the national level (by IAIP/IP) to understand priorities across sectors and nationally. IAIP/IP will also address normalization of criticality criteria with neighbor countries to identify and prioritize CI/KR cross-border assets or

those assets with cross-border implications.

- **Normalization**—IAIP/IP is using the knowledge and expertise of SSAs to assist in the identification and assessment of CI/KR assets within their sectors. However, to support proper resource allocation and consistent performance measurement, data from different sectors must be normalized across sectors to allow a meaningful comparison of risk across sectors. Such cross-sector normalization currently relies exclusively on relatively simple mathematical tools. Looking forward, simple mathematical tools that compute cross-sector analytical results are insufficient because they do not currently include quantitative and objective interdependency information that can significantly impact the vulnerability or consequence-of-loss values assigned to an individual CI/KR, if viewed exclusively within one sector. This approach requires the use of robust analytical tools and methodologies in addition to information provided by SSAs. IAIP/IP is using simple analytical normalization tools based on the assessment methodologies it uses today, and is sponsoring development of more sophisticated tools capable of using the higher-quality data that will be available from the SSAs. Ultimately, the evolving assessment tools used within the sectors will, by design, be compatible with the normalization process so that effective prioritization of assets can be made based on risk, which considers the threat information, the specific vulnerabilities of each asset, and the potential consequences of any event that might occur. IAIP/IP will work with the SSAs to ensure that IAIP/IP will be in the position to use a standardized approach and analytical tools to compare the potential consequences and vulnerabilities of disparate infrastructures, and will share this approach with the SSAs to help them normalize the analyses within their sectors.
- **Risk Analysis**—Risk analysis is the process of applying the general threat assessment to identified vulnerabilities to determine the level of risk. In this case, risk analysis





is broad-based, applying across a wide set of plausible threat scenarios and relying on views of asset (target) attractiveness in light of the general threat environment. It is designed to support the identification of long-term or permanent protective programs for continuous improvement in the sector's risk management performance, particularly for new threat tactics that may have previously been uncovered. In the risk-management framework, this risk analysis may be carried out by the SSAs and asset owners if they have general threat assessments provided by IAIP/IA or their own intelligence groups (e.g., the Transportation Security Administration's intelligence division); or the risk analysis may be carried out by IAIP/IP. These analyses feed into the prioritization process. Risk analyses may also require normalization in order to support cross-sector analyses.

- **Prioritization**—The normalization and risk analysis processes allow SSAs to set priorities for protective programs within the sector, and allows IAIP/IP to set priorities across sectors, segments, regions, and individual sites—depending on the nature of the threat and/or the purpose of the risk analysis. Once assets are prioritized, IAIP/IP will then work with the SSAs and sector stakeholders to guide the allocation of resources for protective actions (short-term) and programs (longer-term). This allocation process will take into account the return on investment of the protective action (i.e., the overall value relative to the overall cost). Strategic prioritizations will change over time, but usually slowly. Additionally, the prioritization can be used to determine resource requirements and funding allocations for various research and development efforts, and to inform international outreach programs.

### 3.3.2 Interdependencies Analysis

As part of the process for “normalizing” across sectors, IAIP/IP conducts the crucial analysis of interdependencies between sectors. Using data that is entered in the NADB, the results of DHS/IP CIP activities, and other input from the SSAs, IAIP/IP continually reviews the relationships between sectors to identify dependencies, where the failure of one sector may result in cascading impacts throughout other sectors. For example, nearly all sectors rely on the service grids of the energy, information technology, telecommunications, and transportation sectors—failures in these crucial service areas can be devastating on the abilities of other sectors to function properly. In some sectors, the dependency may be more localized; for example, the proper functioning of the firefighting services will be dependent on a reliable local water supply. Thus, if the Water Sector is compromised, the ability of the Emergency Services Sector to properly function in that location may also be compromised. Interdependencies can also be the potential for exploitation, (e.g., where one sector is used by a terrorist to attack other sectors.) For example, terrorists may use transportation vehicles or postal and shipping methods to attack another sector. IAIP/IP will be using SSA data on CI/KR assets and their vulnerabilities to continually assess the interdependency relationships among sectors and ensure that these relationships are integrated into the subsequent analyses of risk, which will form the basis for prioritization of protective programs.

Assessment of risk across the CI/KR sectors is not a process that can be addressed in a linear or hierarchical way. While linear analysis is valuable, the greatest value results from analyzing interdependencies across and between sectors, and between asset categories within sectors. By assessing risk in terms of the inter-sector vulnerabilities as well as the cross-sector impact to human, cyber, and physical infrastructures, DHS is able to implement protective measures that truly protect against attacks that could affect the critical infrastructures of multiple sectors. This drives increased efficiency in the deployment of protective measures, better use of resources, and lower overall risk to the Nation through a better understanding of how to protect the ways the infrastructures work together to drive the American economy.

### 3.4 Develop and Implement Protective Programs for CI/KR

The fourth step in the risk management framework is the development and implementation of efficient and cost-effective protective programs. A protective program is a

coordinated plan of action to prevent, deter, and mitigate terrorist attacks on critical assets, as well as to respond to, and recover from, such attacks in a manner that limits the consequences and value of such attacks. Actions to protect an asset fall into one or more of the following general categories:

- **Deter**—Actions that cause the potential attacker to perceive that the risk of failure is greater than that which the terrorist find acceptable. Examples include improved awareness and security (e.g., restricted access, vehicle checkpoints), enhanced police presence, and such cyber-protection features as additional access controls.
- **Devalue**—Actions that reduce the attacker’s incentive by reducing the target’s value. Examples include developing redundancies and back-up systems, or de-emphasizing the importance of a particular event.
- **Detect**—Activities or mechanisms that identify potential attacks, validate the information, and/or communicate the information as appropriate. For specific assets, examples include intrusion-detection systems, monitoring, operation alarms, surveillance detection and reporting, and employee security awareness programs. General detection activities include intelligence gathering, analysis of surveillance activities, and trend analysis of law enforcement reporting.
- **Defend**—Actions that protect assets by preventing or delaying the actual attack. These include physical hardening, buffer zones, fencing, and structural integrity.

In addition to these preventive actions, protective programs may also include actions that have an impact on the consequences, should an attack occur—although this is not the focus of the NIPP. Such actions might include:

- **Mitigate or respond**—Actions that mitigate impacts of an attack, such as having adequate response plans and training
- **Recover**—Actions that allow the sector to resume operations quickly and efficiently, such as developing continuity of operations plans

SSAs’ approaches for working with sector stakeholders to develop long-term protective programs will be further refined as the NIPP is implemented. Across the sectors, these protective programs have certain features in common, as follows:

- **Comprehensive.** In general, the sector-specific protective programs developed under the Interim NIPP are comprehensive; they not only cover the range of actions identified above, but also ensure that protective measures address the physical, human, and cyber aspects of the

sector assets. These programs take into account long-term, short-term, and sustainable protective programs. Furthermore, SSAs have identified or described the range of specific actions that may be employed (e.g., operational changes, physical protection, equipment hardening, backup communications, response plans, and security system upgrades) to protect assets within the sector.

- **Coordinated.** Because of the highly distributed and massive nature of infrastructure sectors, the responsibility for protecting assets must be shared among Federal, State, local, tribal, and private sector stakeholders. In particular, asset owners and operators (public or private) have an inherent responsibility to protect property and people, even if only through increased awareness of terrorist threats and simple operational responses (e.g., changing daily routines) to reduce the vulnerability. SSAs will provide an informed perspective on the most effective long-term protective strategies, and must effectively coordinate the development and implementation of protective programs. For some sectors, there are existing standards/criteria, guidance documents, and tools that are shared among sector stakeholders. State, local, and tribal entities will also be actively involved in the development of protective programs, and will supplement Federal guidance and expertise, and provide specific law enforcement personnel as needed. Finally, IAIP/IP serves as the national focal point for the development and implementation of protective programs for high-risk assets in partnership with these stakeholders.
- **Risk-based.** Development and implementation of protective programs is the fourth step in the risk-based model. Therefore, sector-specific programs will build upon the asset identification, vulnerability assessment, and prioritization activities described in the previous sections of this chapter. Within each sector, the SSA will work with stakeholders to identify the range of protective actions



that could be taken to minimize the vulnerabilities identified; however, to ensure effective use of resources, actual implementation of protective measures will take into account any specific information about the likelihood of plausible threats, so that programs are being developed to account for the wide range of all possible threats. Decisions for implementation will take into account balancing the potential reduction in known risk against the feasibility and affordability of the protective measure (the return on investment). Consistent with the risk-based model, the protective programs will also include plans for feedback, including information on measuring effectiveness, and when and by which entity the protective programs will be updated and refined.

- **Cost effective.** For asset owners and operators, the business case for protection has grown over the past several years. Companies and other owner/operators have increasingly recognized that disruption or destruction can have significant impacts on operational survivability, shareholder value, customer relations, and public confidence. However, investments in protection can be costly and may not be considered necessary by some, particularly for events that may never occur. Therefore, the protective programs developed as the Interim NIPP is implemented will seek to minimize excessive costs by focusing on protective measures that incorporate many of these features:
  - Are simple, low-cost methods
  - Are consistent with best business practices, and are shared among stakeholders using industry and trade association communication mechanisms
  - Propose cost-sharing incentives, market systems, and other methods for encouraging private sector action
  - Build upon current efforts that have proven to be effective
  - Are applicable across assets, while allowing owner/operators to select the measure best-suited to the particular need
  - Rely on self-assessments, where appropriate
  - Are proportional to the risk, threat, vulnerability, and consequence

IAIP/IP will provide additional assistance to the long-term protective programs using a variety of methods, from implementing specific protective measures to training site owners and operators. Specific IAIP/IP support activities include:

- **National Protective Measures Program**—IAIP/IP coordinates this program, which uses inputs from both the

national and sector-specific vulnerability identification and analysis processes to determine and implement appropriate protective actions.

- **Protective security support for communities**—IAIP/IP provides specific advisory support to the protective community (e.g., law enforcement, first responders, etc), including training and exercise support.
- **General protection plans**—IAIP/IP maintains the General Protection Plans, which provide generally accepted standards of protection and protective measures for all major classes of assets and HV/HR event sites. This also includes sharing of lessons learned and best practices from national-level vulnerability assessments to the sectors, law enforcement officials, and the private sector to allow these parties to enhance the protection of assets that are not nationally critical.
- **Cyber solutions**—IAIP/IP develops long-term, multi-sector strategies to address cyber vulnerabilities.
- **Protective Security Advisor Program**—IAIP/IP provides employees who are security and law enforcement professionals to function as liaisons between DHS and the protective community and general public. Their responsibilities are to be knowledgeable about potential targets of value in their assigned areas and to share information and provide technical assistance to local law enforcement and the owners and operators of assets within those areas.
- **International outreach**—IAIP will work with the Department of State to undertake international outreach to foreign nations to encourage the promotion and adoption of best practices, training, and other programs as needed to improve the protection of overseas assets and the reliability of foreign infrastructures on which the United States depends.

Where implementation of protective measures within a sector is essential for national-level security, the SSA may need to seek regulatory options or policy solutions.

### 3.5 Measure Effectiveness

The last step in the CIP risk management framework is the use of performance metrics to determine the effectiveness of infrastructure protection activities. Working with the SSAs and supporting agencies—and through them, the private and public sector owners and operators of critical infrastructure—IAIP/IP is developing performance measures and metrics to align with existing operational performance metrics. Metrics will measure vulnerability-reduction program accomplishments and drive continuous improve-

## Exhibit 7: Core Metrics

Core Metrics	Description
Total # of assets by class	Asset classes will be different for each CI/KR sector. Tracking this will provide the baseline information needed for subsequent metrics.
% of high-consequence assets to total assets	Tracking this will help determine which sectors are in the most need of assessing vulnerabilities. Details of the data underneath this measure should help determine if there are more critical regions, industries, or sectors in terms of potential impact.
% of high-consequence assets that have completed vulnerability analyses	Tracking this will help determine progress in determining which infrastructure assets and sectors are in the most need of protective and preventative programs.
% of high-consequence assets assessed as high risk	Tracking this will help in determining which sectors require programs to increase prevention, protective, response and recovery capabilities. In conjunction with other measures and data on location and ownership of the assets, it can help focus government and private resources on those sectors, regions and industries, with the highest identified risks first.
% of high-consequence assets that have active protective programs to measurably reduce risk	Tracking this, in conjunction with other measures, will help determine where there are potential gaps in program coverage for critical infrastructure assets determined to be high risk.
% of high-consequence assets that have been assessed for readiness, response, and recovery capability	Tracking this will provide insight into the plan effectiveness for readiness, response, and recovery.
% of assets reduced from high risk	Tracking this will provide insight into the effectiveness of the programs implemented to reduce risk. Risk can be reduced through a variety of means, from increasing the difficulty of attacking critical infrastructure assets to decreasing the probability of success of an attack against an asset via a variety of prevention and/or protective measures.

ment of infrastructure protection activities. In addition, both output (e.g., the number of vulnerability assessments performed by a certain date) and outcome (e.g., a reduced number of facilities assessed as high risk, following the institution of protective actions) metrics will be used by the SSAs and DHS to track progress on specific activities outlined in the SSPs. The intent of the measurement process is to provide DHS and the SSAs with feedback on where and how they should focus their resources to be most effective. Measurements will occur at the sector or asset category level, and will not report on individual assets.

Selecting outcome metrics for protective programs is challenging, because risk reduction is not directly observable (i.e., it is often difficult to determine whether a terrorist attack has been avoided or prevented or the extent to which the potential consequences have been mitigated). Relying strictly on output metrics is not adequate to measure the value of infrastructure-protection activities; however, as some SSAs are successfully using outcome metrics to improve their sector-specific programs, DHS intends to identify those best practices and encourage their use in

other sectors as appropriate.

To begin this process, DHS has identified a set of seven core metrics common to all sectors that will be used to evaluate performance. These common core metrics are given in exhibit 7, and are intended to be assessed for each asset class as identified by each SSA for their sector. Each SSA is also working with DHS to develop a set of sector-specific metrics that will supplement the core metrics.

A key element to IAIP/IP's approach to performance measurement will be an annual sector infrastructure protection risk assessment, which will report overall progress against goals for each CI/KR sector. The purpose of this annual risk assessment will be to:

- Act as the overall progress report for each CI/KR sector to track its own progression against infrastructure protection goals (i.e., be a tool used by the SSAs to measure progress)
- Provide a common vehicle among CI/KR sectors for communicating infrastructure protection performance to key stakeholders

- Help to identify best practices from successful programs that can be shared within and among sectors
- Provide feedback to the CI/KR sectors, which will be used as input for the continuous improvement of the NIPP

The sector assessment will be jointly conducted by DHS IAIP/IP and the SSA for a given CI/KR sector. IAIP/IP will provide guidance to SSAs on the format and content for these annual assessments as part of overall guidance on the annual reporting required by HSPD-7. IAIP/IP and the SSAs will engage with private sector stakeholders to determine what role they will play in assisting with these annual assessments. Since the SSPs are currently being developed, the initial sector assessment will establish a baseline for future years.

Longer-term, the sector assessment is intended to be an integrative assessment of success in decreasing the vulnerability or risk to CI/KR by improving key infrastructure protection capabilities: identification of critical assets, assessment of vulnerabilities, protection (including programs to detect, defend, deter, and devalue), response, recovery, and organizational excellence/governance.

### 3.6 Continuous Improvement

Effective and sustainable infrastructure protection will depend on adaptability and continuous improvement of processes and programs. Assuring continuous improvement by capturing learning that results from actions taken, and taking corrective actions to fill gaps as they are identified, requires that a feedback loop become an inherent part of the risk management framework.

Such a feedback loop falls under the overall framework of an information sharing and management system concept, which encompasses the structure of Sector and Government Coordinating Councils (SCCs and GCCs) and their information sharing entities, the partnership with the SSAs and State, local, and tribal entities, and the deployment of the Homeland Security Information Network (HSIN) to these key stakeholders. The term “system” is used in the broadest sense as the structured interaction of people, physical structures, information, and technologies designed to ensure that critical, high-quality, and productive knowledge is provided/available to Interim NIPP decision makers whenever and wherever it is needed. This definition calls for an integrated business process across all key stakeholders at a national level, and provides an integrated view of the sharing and management of information across organizational and technical boundaries.

The SCCs and GCCs represent key portions of the structural foundations for this system, with an inherent feedback loop built into agendas, coordination, and program development, including continuous feedback between and among government agencies, and between the government and Councils. The information sharing entities and the HSIN represent the technical means by which communication and information sharing occur. Other components within this system include structures and processes of communication with intelligence coordination centers within the States, and maintenance of information forums with the State HSAs. Specific application systems, such as the NADB, are viewed as components of this overall system.

As part of the vulnerability reduction program, this system will:

- **Help capture the learning that occurs at the interfaces among organizational components.** The SCCs and GCCs provide forums and interfaces that have not existed before—for instance, between organizational elements within DHS; between DHS, SSAs, and the owners and operators of the Nation’s critical infrastructure; between DHS and the intelligence and law enforcement community; and among the sectors themselves. In such programs, much learning takes place at these interfaces and the formal planning, agendas, and programs of the Councils will help capture lessons learned and incorporate them into future plans and programs.
- **Support the development of and collaboration among communities of practice within the sectors.** The success of infrastructure protection efforts will depend, in large part, on the ability of similar companies within similar industries within sectors to work together on protection. Many of these groupings already exist in industry associations and trade groups. The SCCs and GCCs help strengthen the ability for sharing lessons learned across a sector and across sectors, as well as between government and owners and operators.
- **Support the annual review of learning to make strategic recommendations for the next year.** The concept of operations requires DHS/IAIP to review what has worked well and what has not worked as intended. DHS will work with SSAs and OMB to coordinate the direction of critical infrastructure protection resource allocation decisions and will work with all key stakeholders, including Congress, to develop and implement programs or authorities needed to realize the goal of a self-learning, continuously improving program for infrastructure protection.

# 4. Threat-Initiated Actions

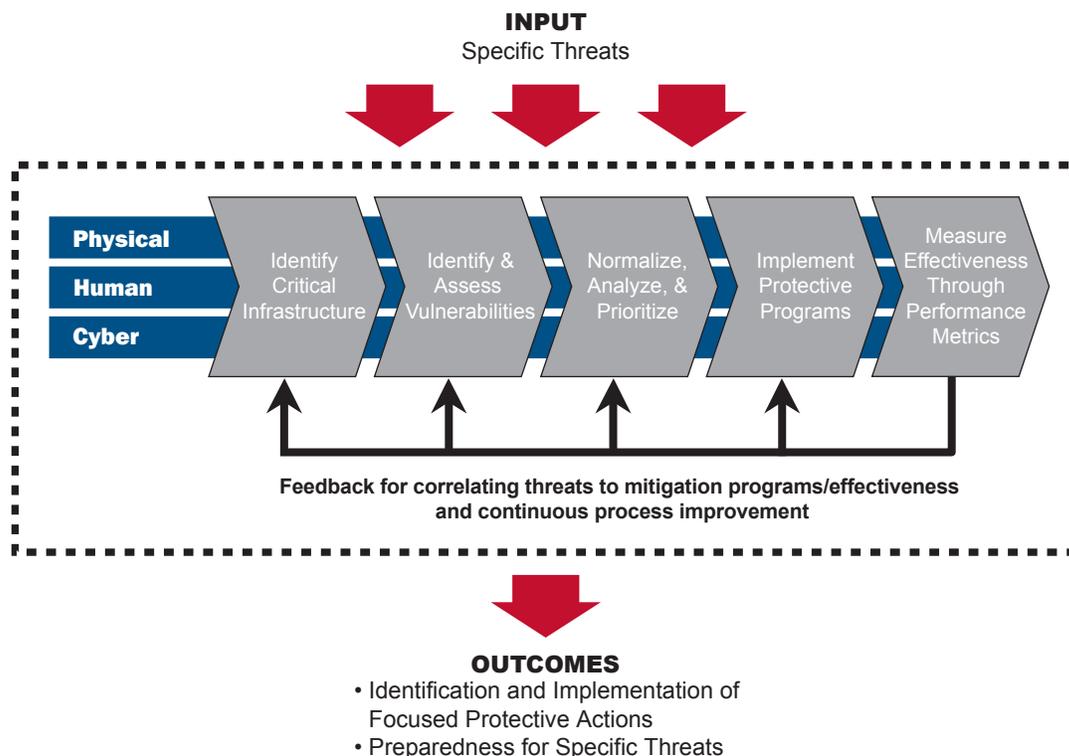
This chapter presents the concept of operations for implementing the risk management framework in response to specific threat information. In this context, DHS reviews existing information on CI/KR or key events, vulnerabilities, and established protective action programs. Based on the results of this analysis and in consultation with relevant stakeholders, as necessary, DHS then issues threat warnings and recommends or undertakes certain protective actions. This has been DHS's primary operating mode since its inception and remains a critical DHS role. Such efforts are constantly informed by IAIP/IA through threat information and intelligence to further understand the risk to specific infrastructure sectors, regions, or specific assets.

Exhibit 8 illustrates the CIP risk management framework as it relates to implementing threat-initiated actions. Under this framework, vulnerability assessments may simply be a review of previously identified vulnerabilities for specific types of assets, or for assets in a particular geographic area; if such results are not available, quick expert reviews may be conducted for specific assets. Established protective programs are reviewed for the completeness of their implementation and the thoroughness of the protection offered against the specific threat(s). Performance measures

may also be reviewed to identify gaps or shortfalls in the implementation of protective programs. Measurement of tactical performance might focus on effectiveness and speed of deployment of new protective actions.

The fundamental inputs to implementation of the risk management framework are threat analyses and warnings. Actionable intelligence is essential for preventing acts of terrorism. The timely and thorough analysis and dissemination of information about terrorists and their activities will

**Exhibit 8: Threat-Initiated Actions**





improve the government's ability to disrupt and prevent terrorist acts and provides useful warning to the private sector and the population.

It is IAIP/IA's responsibility to provide timely analysis and dissemination of current and potential terrorist activities and capabilities, to identify the indicators and precursors of an attack, and to analyze patterns of potential attacks. IAIP/IA pulls together information and intelligence from a variety of sources. IAIP/IA is dedicated to systematically analyzing all information and intelligence on potential terrorist threats within the United States.

The prevention of terrorist acts requires a proactive approach that enhances the capability of policymakers and law enforcement personnel to preempt terrorist plots, warn appropriate sectors, and aid asset owners or operators in taking appropriate protective steps. IAIP/IA fuses and analyzes legally accessible information from multiple available sources pertaining to terrorist threats to the homeland to provide early warning of potential attacks. This information includes foreign intelligence, law enforcement information, and publicly available information. It is a full partner and consumer of all intelligence-generating agencies. By obtaining and analyzing this information, DHS is able to see the dangers facing the homeland comprehensively.

The overall outcome of the tactical implementation of the risk management framework is enhanced preparedness for select CI/KR for specific threats. Once the threat analyses are applied to the risk management framework, the specific outcome of the focused reviews of vulnerabilities and existing protective programs is a set of specific, supplemental, protective actions that should be implemented to address the immediate needs for a subset of CI/KR assets. Such actions are designed to be implemented quickly for specific threats, in contrast to the longer time frame generally needed for the systemic changes necessary to address more inherent vulnerabilities.

The individual steps of the risk management framework are carried out as described below.

#### 4.1 Identify CI/KR

The difference between gathering asset data for ongoing vulnerability reduction, versus in response to specific threats, is generally one of timing and specificity. In response to specific threats, information in the existing inventories is used to identify specific assets and activities that warrant special attention and/or immediate protection, based on current or emerging situations. This has been DHS's primary mode of operation since its inception, as DHS has built up both its knowledge base and its capabilities.

After IAIP/IA or other intelligence determine a specific threat to be credible and make appropriate notifications, IAIP/IP will use the NADB to identify specific assets presenting characteristics that match the threat information, and the vulnerabilities that might be exploited. These characteristics might be related to a geographic location, the potential consequences of an attack, or the interdependencies for the asset. When the threat directly affects cross-border assets, or has implications for neighboring countries, international trade routes, or critical sources for our national infrastructures to function properly, IAIP/IP will work with the Department of State and the international community to identify such assets.

If the asset data are insufficient (e.g., the threat is very different from those previously considered, or the SSAs have not completed their asset data collection efforts), it may be necessary for IAIP/IP to initiate additional information collection actions. Previously, DHS has requested data on high-risk assets directly from state agencies or other sector stakeholders. Going forward, these data requests will be coordinated with the SSAs to avoid redundant or overlapping requests. The intent of the data collection efforts will be to ensure that the most complete and current information is available about assets that may be subject to certain types of threats, so that protective actions are implemented effectively and efficiently. Such data requests are often in response to broad-based increases in threats or intelligence for a particular timeframe.

As with all of the steps in the risk management framework, immediate attention can be provided for one or more assets if needed, without first completing the other steps in the framework. In such instances, IAIP/IP initiates rapid response activities to alert authorities and the protective community (e.g., first responders, law enforcement, secu-

urity, intelligence), and takes action to devalue the target and detect, deter, and defeat the threats. Going forward, such actions will also occur in consultation with the relevant SSAs.

## 4.2 Identify and Assess Vulnerabilities

Threat-initiated vulnerability assessments are focused on assets considered to be at risk because of specific threat information. These assessments are carried out to determine the likelihood of a specific threat's success. As the number and scope of the vulnerability assessments carried out within the sectors, and by DHS as part of the vulnerability reduction program increase, the need for threat-initiated vulnerability assessments may decrease, because the data on vulnerabilities will already be in place when threat information becomes available. IAIP/IP is also in the position to address multiple targets or assets, such as may be found in a particular location, in its assessments.

Generally, IAIP/IP directly carries out any additional threat-initiated vulnerability assessments. Such threat-initiated vulnerability assessments consist of the following activities:

- Obtaining threat assessments from IAIP/IA on the specific threat
- Establishing the vulnerability assessment team
- Identifying physical, human (e.g., procedural), and cyber vulnerabilities that might be exploited under the specific threat, either from reviews of strategic vulnerability assessments or through a combination of field visits and expert assessments
- Analyzing sufficiency of existing protective programs for the specific threat

As discussed in Vulnerability Reduction Program, IAIP/IP also examines interdependencies between sectors to ensure that these crucial relationships are considered as part of the subsequent risk analyses and protective program decisions.

IAIP/IP conducts a risk analysis process, in which it uses existing vulnerability information and applies timely intelligence (e.g., observed indicators of terrorist activity) to determine: (1) potential method of attack; (2) probability of success; and (3) consequences of the attack (including secondary and tertiary effects). By applying this information to the selected subset of assets from the NADB, IAIP/IP can quickly identify the assets at greatest risk to a particular threat—not simply those with the greatest potential consequences or unprotected vulnerabilities.

In the case of particularly high-risk or high-value targets,

IAIP/IP performs a very quick turnaround analysis to identify what assets might be at risk, to allow protective actions to be initiated as quickly as possible. Those involved in site-specific visits and assessments will endeavor to provide immediate assistance to owners and operators of facilities or sites on realizing immediate improvements in their protective readiness, pending receipt of a more-detailed assessment report.

## 4.3 Analyze, Normalize, and Prioritize CI/KR

Threat-initiated analyses can occur daily, weekly, or at any time that the threat information changes, resulting in constantly changing threat-based priorities. The protective actions taken in light of such risk analyses tend to be short-term in nature. Because prioritization results for specific threats are sensitive to the time and reason they were generated, DHS intends to develop listings of prioritized assets only in the context of specific threats, not in general.

## 4.4 Develop and Implement Protective Programs for CI/KR

There are several sectors that, because of their high visibility to terrorists, their high inherent vulnerability, or the highly distributed nature of their infrastructure, are considered the highest risk sectors. For these high-risk sectors in particular, IAIP/IP implements protective measures in response to specific threats and in response to new critical vulnerabilities discovered for new types of threats or attacks. IAIP/IP's activities in this area include: issuing warnings, coordinating the deployment of nonfederal protective resources (e.g., State and local law enforcement), deploying Federal protective resources (e.g., National Guard), and coordinating consequence-management planning, or even evacuations. These



actions may also be taken for other sectors if the analyses of current threat information suggest that particular assets are likely targets.

Although many vulnerabilities have been at least partially mitigated through implementation of buffer zones (e.g., around chemical and nuclear sites) and increased personnel and physical security measures (e.g., for certain transportation systems and soft target sites), additional protective measures are often required. IAIP/IP continually adjusts its focus in response to current threat information and in response to discoveries of new vulnerabilities.

For cyber threats, IAIP/IP's role is more restricted in response to specific threats, relying more on owners and operators to follow IAIP/IP's precautions and implement suggested short-term measures.

## 4.5 Measure Effectiveness

Within the threat-initiated program, performance metrics will be used to constantly improve the alignment of protective programs to the ever-changing threat environment, and to drive higher awareness of the threat environment across CI/KR owners and operators. This process will provide the information necessary to assist senior officials in making informed decisions about protective actions and national risk management on a real-time basis, using a scorecard approach to demonstrate preparedness at a given time for specific threat situations.

The scorecard is used in a threat-specific context, allowing IAIP/IP and other senior-level Federal officials to understand the state of preparedness for a very specific type of threat, at a particular time. As such, any individual scorecard is not necessarily related to any other, unless the threat has stayed constant for some period where the benefits of newly implemented protective programs can be shown. The scorecard reflects the combination of the characteristics of a specific threat, the vulnerabilities of the assets, and the protective programs already in place for those assets.

In addition, if any short-term actions are to be taken to address specific, threat-initiated actions, these programs should include a focused measurement plan. This plan should identify key process and outcome metrics, including key milestones. Time permitting, the plan should also include an independent verification and validation step to test the successful implementation of the threat-specific action (e.g., for a buffer zone protection plan, a penetration test by an independent third party). Finally, a reporting plan should be developed to facilitate tracking of the metrics.

DHS will develop and issue additional guidance on future reporting requirements needed to assess success of the NIPP.

## 4.6 Continuous Improvement

The general system for continuous improvement of infrastructure protection processes was introduced in Section 3.6 of this document. For threat-initiated actions, this system will:

- **Support the continuous evolution of infrastructure protection by providing feedback on the effectiveness of protection.** Infrastructure protection is evolutionary, requiring feedback from each of the five steps in the risk-management framework. Much of this feedback will be structured through the use of performance measures and traditional feedback mechanisms, such as an after-action report on how well a protective measure mitigated the impact of terrorist attack. However, much important learning will not fit neatly into a specific activity or package. An effective system will integrate feedback gathered through traditional channels with learning gathered through other, more informal channels. This feedback will ensure that our infrastructure protection efforts evolve in response to actual—rather than predetermined—needs in the environment.
- **Help to increase the effectiveness and reach of the infrastructure protection resources by developing consolidated responses to daily needs.** Similar learning experiences and responses can point to areas in which infrastructure protection resources can be maximized by developing consolidated response to common needs, removing redundancy, and encouraging resource sharing.
- **Support the movement of and access to information at a variety of places and times.** In a complex program, information must flow in all directions to ensure that required information is available to decision makers when they need it, without getting caught in the planning paralysis that is often associated with top-down planning approaches. Similarly, traditional, transaction-based processes often limit the direction and timing of the information flow. The system will support the flow of information in multiple directions and, at various times, encourage a more open and valuable flow of information among legitimate system stakeholders. It will also capture information and analyses that might otherwise be lost when key staff involved in implementing the risk management framework move to other positions.

# 5. Roles and Responsibilities

This chapter presents the proposed roles and responsibilities of all stakeholders in the implementation of the Interim NIPP, and identifies some mechanisms for coordination and information exchange among stakeholders. The descriptions below are intended to be a starting point for further discussion and engagement with other Federal agencies, the private sector, and State, local, and tribal entities. As the Interim NIPP is implemented, the stakeholders will work together to further evolve specific roles in the national CIP program and the mechanisms that will be used for coordination and information sharing.

## 5.1 Key Responsibilities

Although DHS is responsible for implementing the NIPP, it relies on the participation and cooperation of other Federal departments and agencies to protect the vast national infrastructure. Even more importantly, because the CIP program is a national, not Federal, program, DHS will need the ongoing involvement of private sector owners and operators, and State, local, and tribal entities. The proposed roles and responsibilities of the stakeholders are summarized in exhibit 9 and described in the following sections.

### 5.1.1 Department of Homeland Security

As set forth in HSPD-7, DHS is ultimately responsible for the national CIP program. DHS leads this process, and provides the single point of accountability and coordination to leverage the sector-specific expertise, relationships, and resources of all stakeholders.

As part of its *coordination* role, DHS:

- Coordinates and integrates the relationships among DHS, SSAs, other Federal agencies, the private sector, and State/local/tribal entities
- Promotes voluntary participation in infrastructure protection activities and identifies and explores market-based incentives for consideration by the executive and/or legislative branches of the government
- Develops metrics, gathers data from SSAs, and tracks performance measures for the infrastructure protection program and Interim NIPP implementation
- Following its DHS International Strategy, performs outreach functions with the international community to enhance the sharing of information and to improve the management of international agreements regarding

critical infrastructure protection

In its *leadership* role, DHS:

- Analyzes specific threats, provides threat warnings, and conducts general threat assessments
- Provides consistent policies, approaches, guidelines, and methodologies to assist SSAs and others to carry out infrastructure protection activities (e.g., identifying assets, conducting vulnerability assessments, developing protective programs)
- Provides specific expertise and assistance in addressing physical, human, and cyber elements of CI/KR
- Serves as the lead Federal organization in brokering the information in/information out interface with sector stakeholders
- Sets national critical infrastructure protection priorities

Within the risk-management framework DHS is responsible for the following activities:

#### 5.1.1.1 Threat Assessment

- Provide timely analysis and dissemination of current and potential terrorist activities and capabilities
- Identify the indicators and precursors of an attack
- Analyze patterns of potential attacks
- Receive and analyze law enforcement, intelligence, and other information from Federal, State, and local government agencies (including law enforcement agencies), as well as private sector entities
- Integrate such information in order to:
  - Identify and assess the nature and scope of terrorist threats to CI/KR

Exhibit 9: Key Roles and Responsibilities by Risk Management Framework Stage

	Identify Critical Infrastructure	Identify & Assess Vulnerabilities	Normalize, Analyze, & Prioritize	Implement Protective Programs	Measure Effectiveness
<b>DHS/IAIP/IP</b>	<ul style="list-style-type: none"> <li>Set standards for CI/KR identification and data reporting</li> <li>Maintain national inventory of assets</li> <li>Conduct data calls in coordination with SSAs</li> </ul>	<ul style="list-style-type: none"> <li>Develop consistent approaches &amp; tools</li> <li>Provide expertise</li> <li>Conduct high-risk, cross-sector, &amp; threat-specific assessments</li> <li>Share lessons-learned with stakeholders</li> </ul>	<ul style="list-style-type: none"> <li>Develop guidance &amp; tools for sectors</li> <li>Lead cross-sector normalization &amp; prioritization</li> <li>Analyze interdependencies</li> <li>Update prioritization based on threats</li> <li>Identify R&amp;D needs</li> </ul>	<ul style="list-style-type: none"> <li>Coordinate R&amp;D</li> <li>Promote cross-sector best practices</li> <li>Identify incentives for voluntary implementation</li> <li>Implement selected protective programs for highest risk assets</li> <li>Guide resource allocation</li> <li>Train &amp; exercise</li> </ul>	<ul style="list-style-type: none"> <li>Report on national status</li> <li>Track program implementation</li> <li>Provide feedback</li> </ul>
<b>IA</b>	<ul style="list-style-type: none"> <li>Detect &amp; identify threats to assets</li> </ul>	<ul style="list-style-type: none"> <li>Provide threat assessments</li> <li>Understand threats in light of vulnerabilities</li> </ul>	<ul style="list-style-type: none"> <li>Provide threat information</li> <li>Support updates of prioritization based on threat data</li> </ul>	<ul style="list-style-type: none"> <li>Provide threat warnings</li> </ul>	
<b>SSA</b>	<ul style="list-style-type: none"> <li>Establish criteria for data collection</li> <li>Collect data &amp; develop sector asset lists</li> <li>Coordinate data calls with DHS</li> </ul>	<ul style="list-style-type: none"> <li>Develop approaches</li> <li>Offer tools for self-assessments</li> <li>Assess most critical assets</li> <li>Share results with DHS</li> </ul>	<ul style="list-style-type: none"> <li>Prioritize sector assets &amp; share with DHS</li> <li>Analyze interdependencies &amp; work with other sectors</li> <li>Identify R&amp;D needs</li> </ul>	<ul style="list-style-type: none"> <li>Establish standards</li> <li>Guide resource allocation</li> <li>Identify incentives</li> <li>As needed and appropriate, seek regulatory options</li> <li>Train &amp; exercise</li> <li>Identify R&amp;D needs</li> </ul>	<ul style="list-style-type: none"> <li>Report on sector status</li> <li>Track progress</li> <li>Take corrective actions</li> <li>Provide feedback on progress &amp; gaps/ weaknesses</li> </ul>
<b>Other Federal Agencies</b>	<ul style="list-style-type: none"> <li>Identify assets where applicable</li> <li>Share data &amp; past efforts with SSAs</li> </ul>	<ul style="list-style-type: none"> <li>Provide expertise</li> <li>Support SSAs</li> </ul>	<ul style="list-style-type: none"> <li>Provide expertise &amp; support SSAs</li> <li>Inform cross-sector prioritization efforts</li> </ul>	<ul style="list-style-type: none"> <li>Promote best practices</li> <li>Guide resource allocation</li> <li>Identify incentives</li> <li>As needed, seek regulatory options</li> <li>Identify R&amp;D needs</li> </ul>	<ul style="list-style-type: none"> <li>Share data</li> <li>Provide feedback</li> </ul>
<b>State, Local, and Tribal Agencies</b>	<ul style="list-style-type: none"> <li>Identify assets</li> <li>Share data with DHS &amp; SSAs</li> <li>Respond to data calls</li> <li>Verify &amp; update data based on knowledge &amp; observations</li> </ul>	<ul style="list-style-type: none"> <li>Conduct &amp; share assessments with SSAs &amp; DHS</li> <li>Verify assessments</li> </ul>	<ul style="list-style-type: none"> <li>Identify interdependencies</li> <li>Inform cross-sector prioritization efforts</li> </ul>	<ul style="list-style-type: none"> <li>Supplement private sector capabilities in response to threats</li> <li>Develop State or local level strategies &amp; best practices</li> <li>Identify R&amp;D needs</li> </ul>	<ul style="list-style-type: none"> <li>Share data with SSAs &amp; DHS</li> <li>Track performance where applicable</li> </ul>

Exhibit 9: Key Roles and Responsibilities by Risk Management Framework Stage (*continued*)

	Identify Critical Infrastructure	Identify & Assess Vulnerabilities	Normalize, Analyze, & Prioritize	Implement Protective Programs	Measure Effectiveness
Private Sector	<ul style="list-style-type: none"> <li>Identify assets</li> <li>Provide information on assets to SSAs</li> <li>Respond to data calls from DHS &amp; SSAs</li> </ul>	<ul style="list-style-type: none"> <li>Conduct &amp; share self-assessments with SSAs &amp; DHS</li> <li>Provide expertise to SSA &amp; DHS</li> </ul>	<ul style="list-style-type: none"> <li>Identify interdependencies</li> </ul>	<ul style="list-style-type: none"> <li>Identify existing measures</li> <li>Share best practices</li> <li>Implement minimum standards</li> <li>Help to develop incentive programs</li> <li>Identify R&amp;D needs</li> <li>Support industry initiatives</li> </ul>	<ul style="list-style-type: none"> <li>Track performance &amp; share data with SSAs &amp; DHS</li> </ul>

Note that these roles and responsibilities are supported by a range of stakeholder relationship and information sharing processes.

- Detect and identify threats of terrorism against CI/KR
- Understand such threats in light of actual and potential CI/KR vulnerabilities
- Disseminate the information to affected SSAs and other Federal agencies.

#### 5.1.1.2 Asset and Vulnerability Identification

- Maintain and continually update the NADB of CI/KR and high-profile events
- Conduct periodic data calls to obtain information from sectors regarding potentially high-risk assets or events
- Incorporate information on vulnerabilities and protective actions into the NADB
- Continually review the universe of assets to identify those requiring further analysis and/or action in response to specific threats
- Conduct vulnerability assessments for selected assets in the NADB (either based on high-risk potential or specific threat information)
- Assist SSAs, other Federal agencies, private sector owners and operators, and State, local, and tribal entities in conducting vulnerability assessments by providing tools and guidance
- Collect and maintain information on vulnerability assessment data provided by SSAs, other Federal agencies, or the

private sector

- Develop and distribute Characteristic and Common Vulnerabilities and Potential Indicators of Terrorist Activity reports

#### 5.1.1.3 Cross-Sector Analysis and Prioritization

- Using vulnerability assessment data provided by SSAs and the private sector, analyze for additional, unidentified interdependencies and cross-sector impacts
- Normalize assessment results across sectors
- Conduct analysis of vulnerabilities to prioritize assets based on application of specific threat information to a subset of the asset data
- Use analytical results to identify potential research and development (R&D) needs

#### 5.1.1.4 Protective Programs

- Use prioritization results to guide the allocation of resources for protective programs for DHS and SSA activities
- Develop and implement protective measures for national, high-risk assets
- Identify cross-sector best practices from the data provided by the SSAs, other Federal agencies, and the private sector
- Conduct cost-benefit analyses for new protective programs

- Offer and/or coordinate training and conduct exercises
- Maintain relationships and coordinate with State HSAs to implement protection programs, and to coordinate response programs and dissemination of alerts, warnings, and advisories

#### 5.1.1.5 Information Exchange

- Develop, implement, and expand information-sharing strategies
- Notify the SSAs, other Federal agencies, the protective community, and/or asset owners and operators regarding the need to take action for potentially high-risk assets or situations
- Share lessons learned and best practices regarding vulnerability assessment methods and results with SSAs, sector information-sharing entities, and other appropriate parties
- Serve as private sector liaisons where the SSAs do not have established relationships, and support all SSAs in their outreach efforts to other stakeholders
- Maintain situation and operational awareness of the sectors to support sector-specific and cross-sector protective and response programs
- In conjunction with the Department of State and other Federal departments and agencies, share appropriate information with the international community



#### 5.1.2 Sector-Specific Agencies

The role of the SSAs is to provide the subject matter and industry-specific expertise and relationships to ensure protection of the specific sectors to which they are assigned.

To support the various activities and processes called out in the SSPs, each SSA must establish or identify an organization to carry out those responsibilities. For some sectors, the SSA has a long-standing role in providing leadership to ensure protection of the sector, and will already have the appropriate expertise and organizations in place with appropriate responsibilities, communications, and accountability. For such SSAs, existing regulatory structures often already address many of these issues, and should be leveraged. Other SSAs must establish and maintain new organizational units for this effort. The level of staffing and extent of expertise required will vary significantly, depending on whether the sector relies more on self-assessments or Federal-led assessments, the number and diversity of stakeholders, the method by which data are collected and stored, the number and complexity of interdependency analyses and other broad-based sector studies, and how heavily the SSA relies on the sector participation and IAIP/IP staff, among others. As the Interim NIPP is implemented, the roles and responsibilities of the SSAs will be further developed and refined.

As described in more detail in chapters 1 and 2, and ultimately in the SSPs, SSAs must carry out most or all of the following activities in order to successfully protect its sector's assets:

##### 5.1.2.1 Sector Outreach

- Inventory stakeholders and develop contact databases for outreach efforts
- Develop a stakeholder communication process
- Establish and maintain relationships with all stakeholders or stakeholder groups (e.g., through industry associations and coordinating councils)

##### 5.1.2.2 Asset and Vulnerability Identification

- Working with the sector asset owners and operators, identify the CI/KR within the sector
- Collect and store up-to-date asset data, and make the necessary data accessible to DHS
- Support data calls from DHS regarding high-risk assets
- Establish and disseminate standards, methods, and guidance (as needed)
- Evaluate and maintain vulnerability and risk assessment
- Staff vulnerability assessment teams (as needed)
- Collect, review, and store self-assessment results
- Provide assessment results to DHS (in accordance with law)

### 5.1.2.3 Sector-Specific Analysis and Prioritization

- Conduct sector-level analyses for interdependencies, potential consequences, and other critical issues
- Normalize and prioritize sector assets for making decisions about protective programs
- Provide DHS with analytical results suggesting potentially high-risk assets within the sector

### 5.1.2.4 Protective Programs

- In coordination with DHS, develop and implement protective programs for high-priority assets
- Identify and communicate best practices for protective programs for all critical assets
- Establish minimum standards for protective programs by asset class for implementation by asset owners or operators
- Make decisions about resource allocations for protecting different sets of prioritized assets (for resources within their control)
- Identify regulatory options for protective measures, as needed and allowed by law
- Promote initiatives to develop additional protective programs or for the application of such programs from other sectors within the sector
- Offer training and conduct exercises (as needed)

### 5.1.2.5 Information Exchange

- Establish metrics and gather the required data to keep metrics current
- Track performance measures to identify progress within the sector and provide current information to DHS
- Provide feedback to the stakeholders on progress and perceived gaps and weaknesses
- Report annually on activities and progress
- Contribute to annual R&D plan development
- Request funding to implement the plan, for select initiatives, and for high-priority R&D efforts
- Communicate with other SSAs
- Exchange information with the international community, as appropriate

### 5.1.3 The Private Sector

As the owners and operators of the majority of assets, private sector firms engage in risk management planning and invest in security as a necessary business function. They also remain



the first line of defense for their own facilities, and, in some cases, serve as first responders. In order to make immediate improvements in CIP, implementing the Interim NIPP, the CI/KR private sector owners and operators will be encouraged to follow the guidance jointly outlined by SSAs, DHS, other Federal agencies, State, local, and tribal entities to:

- Use sector leadership coordinating entities to cooperate with others in the sector to identify and promulgate suggested desirable practices and procedures, and evolve these over time to accepted best practice standards, develop performance metrics, develop information-sharing mechanisms and procedures, ensure cross-sector coordination and communication, etc.
- Participate in information exchanges among themselves and with government
- Identify potentially critical assets and share information with the SSAs and DHS
- Conduct self-assessments of vulnerabilities and share select information
- Identify existing protective measures
- Implement additional protective programs to achieve minimum guidelines
- Work with Federal departments and agencies to develop incentive programs to encourage voluntary implementation of protective measures
- Respond to changes in threat levels
- Monitor and track performance
- Share analysis of actual physical or cyber attacks to enhance protective programs

- Help the SSAs to identify R&D needs
- Undertake certain initiatives individually or through trade associations to fill key methodological gaps or technological needs

The National Infrastructure Advisory Council, the Homeland Security Advisory Council, and the Private Sector Advisory Committee provide important advice to and review of IAIP/IP's infrastructure-protection activities. These councils also provide an engaged mechanism to vet new programs, such as the private sector best practices program, to a group of executive-level leaders to obtain feedback on the direction of new infrastructure protection programs to receive suggestions for increasing the adoption or success of these programs.

### 5.1.4 State, Local, and Tribal Entities

Certain CI/KR, State, local, and tribal entities may serve as owners or operators for a significant portion of the sector. State, local, and tribal entities also play a large role in planning and implementing detection, prevention, and mitigation programs within the communities where CI/KR are located. They constitute the front line of response and defense in support of the security spectrum, and States act as conduits for requests for Federal assistance when the threat exceeds local and private sector capabilities.

In terms of the risk management framework, State, local, and tribal entities also are involved in:

- Identifying CI/KR and assessing vulnerabilities. For example, as part of their own CI/KR efforts, States conduct vulnerability, risk, and needs assessments
- Responding to “data calls” from DHS to identify high-priority assets or events
- Developing and implementing Statewide homeland security strategies
- Helping the SSAs and DHS to verify asset or vulnerability data
- Implementing their own programs that involve CI/KR asset identification, vulnerability assessment, or protection
- Providing updates in asset information based on onsite or onscene observations
- Supporting or implementing protective measures (e.g., through onsite presence of law enforcement)

### 5.1.5 Other Federal Agencies

Specific Federal departments and agencies not designated as SSAs have special functions in infrastructure protection.

Paragraphs 22 and 29 of HSPD-7 identify specific responsibilities for certain departments and agencies, including the following:

- The Department of State, in conjunction with DHS and the Departments of Justice, Commerce, Defense, and Treasury, works with foreign countries and international organizations to strengthen CI/KR protection.
- The Department of Justice reduces domestic terrorist threats, and investigates and prosecutes actual or attempted attacks on CI/KR.
- The Department of Commerce works with DHS and private sector, research, academic, and government organizations to improve technology related to CI/KR protection.
- The Department of Transportation and DHS collaborate on all matters related to transportation security and transportation infrastructure protection. The Department of Transportation is responsible for operating the national air space system. DOT and DHS will collaborate on regulating the transportation of hazardous materials by all modes (including pipeline).
- The Nuclear Regulatory Commission works with DHS to ensure the necessary protection of commercial nuclear reactors for generating electric power and non-power nuclear reactors used for research, testing, and training; nuclear materials in medical, industrial, and academic settings and facilities that fabricate nuclear fuel; and the transportation, storage, and disposal of nuclear materials and waste.

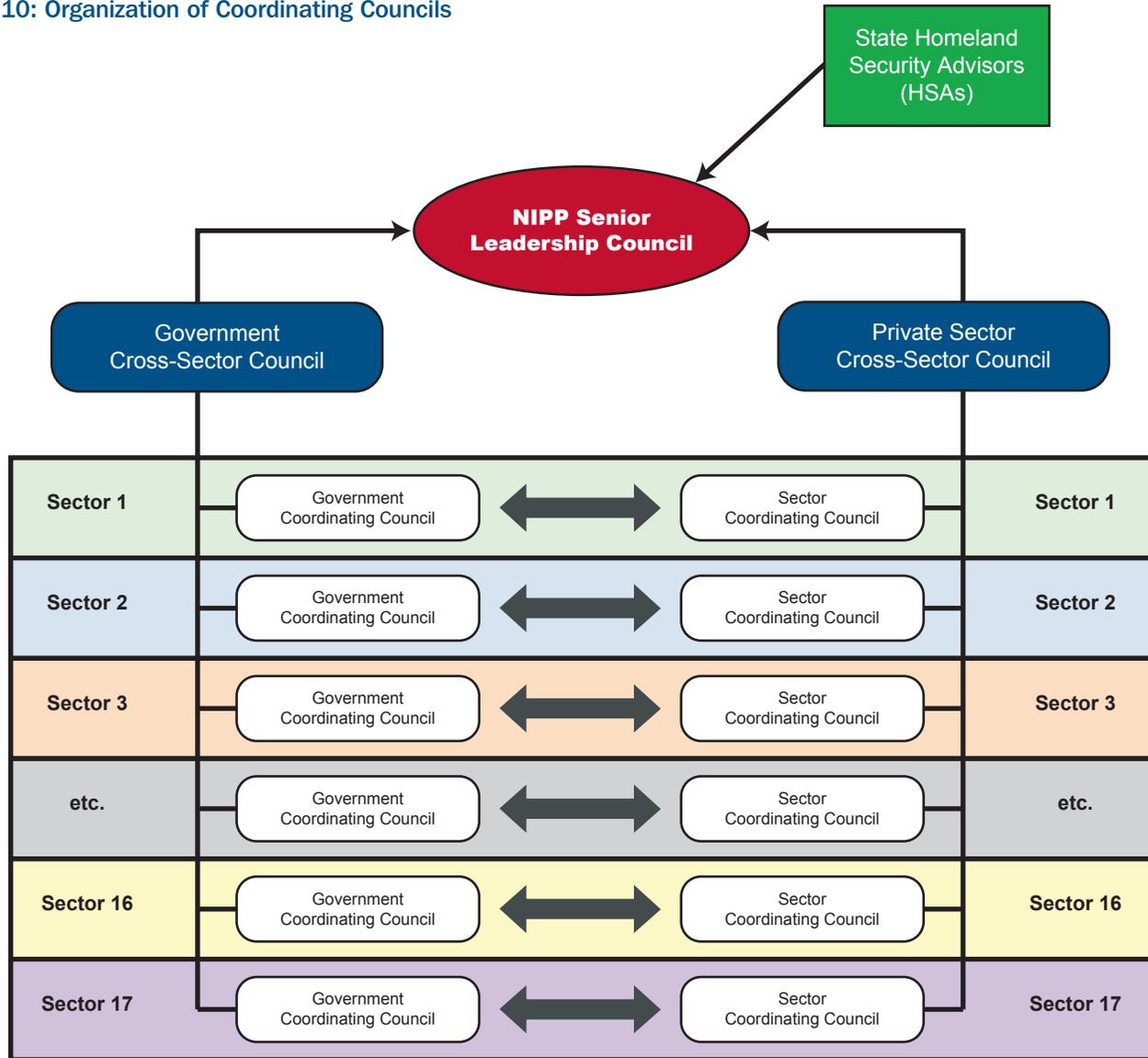
In addition, Federal departments and agencies may provide information on aspects or parts of a particular sector; may identify and assess the potential vulnerabilities and consequences for a particular sector; or may play a role as the regulatory agency for many owners and operators represented in the sector.

## 5.2 Leadership and Coordination Mechanisms

For the national CIP program to be successful there must be efficient and effective partnership, communication, and coordination among DHS, SSAs, other Federal departments and agencies, private sector owners and operators, and State, local, and tribal entities. This section describes the following coordination mechanisms:

- The NIPP Senior Leadership Council and the Cross-Government and Cross-Sector Coordinating Councils
- CI/KR Sector Coordinating Councils (SCCs), which are

Exhibit 10: Organization of Coordinating Councils



self-organized, private sector-led mechanisms that facilitate coordination within the sector and with appropriate government stakeholders

- CI/KR Government Coordinating Councils (GCCs), which support the sector by coordinating among government stakeholders and interfacing with the SCCs
- Mechanisms and tools to support the coordination mechanisms
- Integration of Federal, State, local, and tribal entities into sector activities

### 5.2.1 NIPP Leadership Councils

To enhance communication and coordination between and among Federal departments and agencies, State HSAs,

and the private sector, DHS will establish a NIPP Senior Leadership Council (NIPP Council). The NIPP Council will serve as a resource to provide advice, information, and recommendations on issues associated with the continuous operational enhancement of the NIPP (including the SSPs). The NIPP Council will lead, integrate, and coordinate the execution of the NIPP through the GCCs and the SCCs as depicted in exhibit 10.

The Cross-Government Coordination Council will comprise all the SSA leaders. The leadership representatives from the individual CI/KR GCCs will come together to form a government cross-Government Coordination Council to address common and cross-sector interdependency and policy issues.



The Cross-Sector Coordination Council will comprise private sector leaders from the individual CI/KR SCCs and will address common and cross-sector interdependency issues.

### 5.2.2 Sector Coordinating Councils

Sector Coordinating Councils are being established by the private sector for the Nation's CI/KR sectors. The purpose of the SCCs is to provide the framework for private-sector owners and operators to engage DHS and the SSAs and to collaborate with them to (1) identify, prioritize, and coordinate the protection of CI/KR, and (2) facilitate sharing of information about threats, vulnerabilities, incidents, potential protective measures, and best practices.

The CI/KR SCCs provide a coordination framework for the private sector owners and operators, and they represent a single point of entry for the sector to internally coordinate on the entire range of infrastructure protection activities and issues. The primary function of an SCC is to:

- Facilitate inclusive organization and coordination of the policy development, infrastructure-protection planning, and plan implementation activities within the sector. Such activities include broad-based planning; development of suggested practices and evolution of these practices over time to best-practice standards; promulgation of programs and plans; and development of requirements for effective information sharing, research and development, and cross-sector coordination.
- Identify and support the information-sharing mechanisms and capabilities (e.g., ISACs) deemed most appropriate for the sector. The core function of these information-sharing mechanisms and capabilities is to deliver alerts, warnings, and advisories to the sector and to share back with DHS and the SSAs information on both threats and incidents.

### 5.2.3 Government Coordinating Councils

DHS and the SSAs will implement a CI/KR Government Coordinating Council for each sector, as a government counterpart to the private sector SCC. Each GCC will comprise representatives from DHS, the SSA, and the appropriate supporting Federal departments and agencies.

The core function of each CI/KR GCC is to:

- Provide interagency coordination at the sector operating level through partnership among DHS; the SSA; and other supporting Federal departments and agencies
- Coordinate communication, issues development, and resolution among government entities and between the government and the sector
- Coordinate with and support efforts of the CI/KR SCC to plan, implement, and execute sufficient and necessary security to support the Nation's homeland security mission

### 5.2.4 Coordination Support Mechanisms

The activities of the CI/KR sector and GCCs will be supported by information sharing and DHS developed communication mechanisms to ensure that protection programs are operationally coordinated, and that threat and other security-related information is shared with appropriate stakeholders, including the private sector; State, local, and tribal entities; other Federal agencies; and the international community. These mechanisms include the following:

- **Homeland Security Operations Center (HSOC)**—The HSOC is the primary national hub for domestic incident management operational coordination and situational awareness. It is the coordination mechanism by which DHS gathers and communicates operational information to Federal, State, and local authorities and to the private sector. IAIP ensures that HSOC procedures include those related to access and dissemination of Interim NIPP information.
- **Homeland Security Information Network (HSIN)**—The HSIN is a national communication platform and set of capabilities that allows the flow of real-time information among Federal, State, local, tribal, and private sector partners at the Sensitive-but-Unclassified level. The platform provides for such features as alerts, warnings, and advisories dissemination; real-time planning and problem-solving; and information storage, search, and retrieval. DHS is providing access to State homeland security leadership, law enforcement, and emergency managers. The HSIN will also be extended to CI/KR owners and operators to enhance and expand upon the existing information-shar-

ing capabilities between government stakeholders and the owners and operators. The ability of these communities to share a common platform and tools enhances situational awareness, information sharing, and collaboration across the 50 States, U.S. territories, and major urban areas. The HSIN is intended to support and complement CI/KR sector-specific information-sharing activities. Because each sector is unique in its operation and cultural norms, DHS in conjunction with the SSAs, will support the CI/KR owners and operators in developing sector-specific requirements, procedures, and operating structure to effectively use and leverage the HSIN, and to efficiently improve information sharing within the sector; across sectors; and with Federal, State, local, and tribal government agencies.

- **National Infrastructure Coordinating Center (NICC)**—DHS established the NICC in February 2004 to continuously assess the status of the Nation’s critical infrastructure and key resources. The NICC is a 24-hour watch operations center functioning and as extension of the HSOC. Through the NICC, DHS conducts the following:
  - Maintains infrastructure situational and operational awareness, and assesses key resources, including developing and maintaining the tools and databases necessary to assess the nation’s CI/KR
  - Shares information across and between infrastructure sectors by serving as the HSOC infrastructure monitoring component, collecting and sharing infrastructure-related information with the HSOC, DHS, and private industry partners
  - Triages, assesses, and coordinates response to infrastructure incidents and events
  - Conducts and participates in tests and exercises to coordinate sector preparedness
- **United States-Computer Emergency Readiness Team (US-CERT)**—US-CERT is a partnership between DHS and the public and private sectors. Established to protect the Nation’s Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the Nation, and provides a mechanism for sharing information in this area. US-CERT is intended to complement CI/KR sector-specific cyber security information sharing activities.
- **Advisory Councils**—The Homeland Security Advisory Council (HSAC), National Infrastructure Advisory Council (NIAC), National Security Telecommunications Advisory Council (NSTAC), and Private Sector Advisory Committee provide advice, recommendations, and expertise to the

government on infrastructure protection policy and activities. These bodies also focus on enhancing public-private partnerships and information sharing. The councils and committee provide mechanisms to engage with a preexisting group of private sector leaders to obtain feedback on the direction of infrastructure protection programs, and suggestions for increasing the success of these programs.

### 5.2.5 State, Local, and Tribal Government Coordination

Engagement with State, local, and tribal entities also is an important element to ensure effective protection within the CI/KR sectors. State, local, and tribal entities provide the front line of response and protection for CI/KR and are the conduits for requests for Federal assistance when the threat exceeds local and private sector capabilities. The HSAs for each State serve as the key coordination mechanism for IAIP. Through the HSAs, IAIP currently works closely with State, local, and tribal entities to understand cost issues, protective measure implementation, and specific actions needed in response to a direct threat.

Under the HSIN initiative described above, DHS will share information at all levels of State, local, and tribal government. The HSIN provides access to governors, mayors, HSAs, State National Guard offices, emergency operations centers, first responder and public safety departments, and other key homeland security partners. Each receives software licenses, technology, and training to participate in combating terrorism, information sharing to combat terrorism, and increase antiterrorism situational awareness.

The SSAs also work closely with their particular counterpart State, local, and tribal government agencies to address sector-specific issues. In implementing the Interim NIPP, these relationships should continue to be used and strengthened, particularly through the GCCs. In situations where SSAs need to coordinate with State or local governments outside of existing relationships, they may utilize the DHS Office of State and Local Government Coordination and Preparedness to facilitate the communication.

# 6. Integration with Other Plans

As required by paragraph 27 of HSPD-7, this section of the Interim NIPP describes how the Plan relates to the National Strategy, the National Response Plan, and other Federal emergency preparedness and response programs, as well as other activities and implementation requirements under HSPD-7 and other directives.

The National Strategy and the Homeland Security Act of 2002 served to mobilize and organize the Nation to secure the homeland from terrorist attacks. The DHS Strategic Plan identifies seven goals that guide the overall efforts of the Nation in realizing a more secure and ready state. These goals are:

1. **Awareness:** Identify and understand threats, assess vulnerabilities, determine potential impacts, and disseminate timely information to our homeland security partners and the American public.
2. **Prevention:** Detect, deter, and mitigate threats to our Nation.
3. **Protection:** Safeguard our people and their freedoms, CI/KR, property, and the economy of our Nation from acts of terrorism, natural disasters, or other emergencies.
4. **Response:** Lead, manage, and coordinate the national response to acts of terrorism, natural disaster, or other emergencies.
5. **Recovery:** Lead national, State, local, and private sector efforts to restore services and rebuild communities after acts of terrorism, natural disasters, or other emergencies.
6. **Service:** Serve the public effectively by facilitating lawful trade, travel, and immigration.
7. **Organizational excellence:** Value our most important resource— our people. Create a culture that promotes a common identity, innovation, mutual respect, accountability, and teamwork to achieve efficiencies, effectiveness, and operational synergies.

The NIPP predominately deals with awareness, prevention,



and protection. However, asset information, vulnerability assessment, and information on the protective action programs, combined with the information-sharing capabilities established through the NIPP and associated SSPs, become an operational capability upon the activation of components of the National Response Plan.

## 6.1 National Response Plan (NRP)

The purpose of the NRP is to establish the single, comprehensive approach required to enhance the ability of the United States to respond to domestic incidents. The NRP forms the basis for the mechanism whereby the Federal Government coordinates its interface with State, local, and tribal entities and the private sector. It establishes incident management protocols to help protect the Nation from terrorist attacks and other natural and manmade hazards; save lives; protect public health, safety, property, and the environment; and reduce adverse psychological consequences and disruptions to the American way of life.

The NRP applies to all Incidents of National Significance<sup>11</sup>—those high impact events that require a coordinated and effective response by an appropriate combination of Federal,

<sup>11</sup> Based on the criteria established in Homeland Security Presidential Directive-5, "Management of Domestic Incidents," February 2003.

State, local, tribal, private sector, and nongovernmental entities to save lives, minimize damage, and provide the basis for long-term community recovery and mitigation activities. The intent of the NRP is to ensure full integration and seamless transition as the response to an Incident of National Significance progresses.

The NIPP supports the NRP during the prevention phase by providing information on critical assets, vulnerabilities, and protection programs. Through SSA and DHS interpretation of data, NRP response planning is informed by the most current and accurate assessments of CI/KR vulnerabilities. The primary agencies for the Emergency Support Functions identified in the NRP are to access the information capabilities of the NIPP as they pertain to the response capabilities of the Emergency Support Function. IAIP serves as the coordination mechanism through which the infrastructure protection framework as presented in the NIPP can inform the NRP and other Department and Agency response plans regarding the status and vulnerabilities for the CI/KR.

During the preparedness phase, the NIPP supports the NRP by providing data on critical assets within geographical areas, and the assessed vulnerability of those assets at the time of perceived threat. Response organizations can be directed through the NRP structure to prepare for response based on the anticipated consequences of a realized incident.

During the response phase of an incident, the information derived from NIPP implementation can be used to support initial response capabilities under the NRP. During an Incident of National Significance, DHS/IAIP may designate an Infrastructure Liaison to serve as the principal advisor to the NRP response structure regarding all national and regional CI/KR related issues. In the absence of real-time incident information, the NIPP data can be modeled to provide anticipated consequences, and initial resources can be activated and deployed based on those predictions. As operational assessments are communicated from the field, deployment adjustments can be made, as appropriate.

NRP recovery activities benefit from a centralized listing of CI/KR assets by geographic area, and a mechanism for coordinated damage assessment, available through the NIPP. The NRP emergency response planning mechanism can use this information to prioritize recovery actions and resources.

## 6.2 National Incident Management System (NIMS)

NIMS provides a consistent nationwide approach for Federal, State, and local governments to work together



effectively and efficiently to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. NIMS is an integral component of the NRP and establishes a single, comprehensive system for incident management that, when implemented, will enhance cooperation among departments and agencies at all levels of government. To provide for interoperability and compatibility among Federal, State, and local capabilities, the NIMS includes a core set of concepts, principles, terminology, and technologies covering the incident command system; multi-agency coordination systems; unified command; training; identification and management of resources (including systems for classifying types of resources); qualifications and certifications; and the collection, tracking, and reporting of incident information and incident resources. The Interim NIPP critical infrastructure information will be shared through the NIMS-established communications mechanisms during incident response.

## 6.3 Other HSPD-7 Requirements

The Interim NIPP is related to, but distinct from, the following plans that are also required under HSPD-7.

### 6.3.1 SSA Annual Plans

Under paragraph 35 of HSPD-7, the SSAs must report to DHS on the effort to identify, prioritize, and coordinate protection of CI/KR in their sectors. These annual updates will be the means by which SSAs report progress on implementation of their SSPs. It is the responsibility of IAIP to coordinate with the SSAs to ensure timely and accurate updates of the SSPs.

### 6.3.2 Internal Federal Plans

Under paragraph 34 of HSPD-7, all Federal departments and agencies were instructed to submit to the Director of OMB for approval plans for protecting the physical and cyber critical infrastructure and key resources that they own and operate. Per OMB's implementing guidance (M-04-15, dated June 17, 2004) DHS will coordinate an interagency review of these plans. DHS will prepare a written evaluation of each agency's physical security plan. Agency cyber security plans will be reviewed in a manner consistent with reviews of cyber security reports submitted under the Federal Information Security Management Act.

### 6.3.3 Research and Development Plan

The Nation's CI/KR assets can be protected from acts of terrorism, natural disasters, or other high-impact emergencies by deploying tools, technologies, and systems that reduce risks and mitigate the consequences of an event. Specifically, protection involves:

- Enhancing our knowledge base of critical infrastructure attributes, systems, and technologies that addresses them singly and in an integrated form regarding their functions, reliabilities, vulnerabilities, and interdependencies
- Improving processes for identifying and addressing gaps in current scientific and technological capabilities required to protect CI/KR and minimize impact of disastrous events
- Improving decision-support tools to continuously monitor asset integrity and viability, in order to increase reliability, minimize loss, and maximize safety in natural and overt events
- Supporting the prioritization of securing the components of CI/KR and reducing CI/KR vulnerabilities and consequences of events
- Anticipating the threat/event scenarios, predicting the consequences, and developing proactive measures against the threats/events



All of this must be based on technical and operational requirements from Federal departments and agencies, State and local governments, and infrastructure owners and operators—a partnership among government, industry, and international entities must catalyze development of technologies needed for the protection of critical infrastructures.

HSPD-7 establishes responsibilities for coordinating interagency R&D to enhance protection of CI/KR through development of these tools, technologies, and systems. Under HSPD-7 paragraph 30, DHS, in coordination with the Office of Science and Technology Policy (OSTP), will prepare an annual Federal R&D plan in support of the directive. The DHS Science and Technology (S&T) Directorate and OSTP are leading the development of the first annual Federal R&D plan, in coordination with the Interagency Infrastructure Subcommittee of OSTP's National Science and Technology Council.

A wide range of threats against the many different types of CI/KR assets creates a collection of fundamental strategic concerns for CIP R&D activities. For example, access to an asset can be denied, the use of an asset can be prevented (e.g., if it cannot be operated or controlled, or is contaminated or destroyed), operations can be disrupted (e.g., loss of function), or a supply chain can be disrupted (e.g., by interfering with the input and output flow of raw materials, products, supplies, parts, or information). To address these concerns, a set of nine S&T themes have been identified that capture science and technology needs for critical infrastructure protection in generic areas and cut across infrastructure sectors. These nine CIP R&D themes are:

1. **Detection and Sensor Systems**—Selection, placement, and integration of such systems into CI/KR of all kinds
2. **Protection and Prevention**—Devices, methods, and processes that prevent damage or destruction of critical assets and their interconnections
3. **Entry and Access Portals**—Devices, systems, and methods that control access to critical assets
4. **Insider Threats**—Profiling, detection, anticipation, and monitoring of activities of trusted persons or automated entities within a critical asset, whether central or distributed
5. **Analysis and Decision Support Systems**—Tools to analyze complex situations found in terrorist attack scenarios and decision-support tools for all levels of government authority directed at assets and the interdependencies between them
6. **Response, Recovery and Reconstitution**—Systems,



emergencies, determine appropriate responses, and analyze interdependencies among sectors. Such tools will also be needed to quantify, evaluate, and measure security, to support the business case for protection investments.

- Securing the protocols that underlie the CI/KR sectors—Security controls must be built into the current protocols associated with Internet communications, as well as protocols used by process-control systems (e.g., Supervisory Control and Data Acquisition [SCADA] and other digital control systems).

devices, and processes that support first responders, rescuers, and those rebuilding both temporary and permanent replacements of damaged assets, and the planning systems for all such efforts

#### 7. New and Emerging Threats and Vulnerabilities—

Methods and processes that allow early discovery of emerging threats and vulnerabilities or the abilities of adversaries to pursue new threat forms

#### 8. Advanced Infrastructure Architectures and System Designs—

Development of new technology that addresses current and future infrastructure needs with replacements that have inherently secure foundations

#### 9. Human and Social Issues—

Research into behavioral issues related to victim response and infrastructure operator actions to enhance understanding and decision making during an event

In addition, there are strong linkages to other R&D efforts that address prevention of terrorism, countermeasures to specific threats (e.g., chemical, biological, radiological, nuclear, and explosive [CBRNE]), emergency response, and standards, among others.

The S&T has identified a number of R&D requirements that must be met in order to effectively protect critical infrastructure, both within and across sectors. Key areas include:

- Modeling, simulation, and analysis for real-time decision support and planning—Improved modeling capabilities are needed to simulate natural and terrorist-induced

- Addressing the insider threat—Various tracking, logging, and behavior-based techniques are needed to protect against and make detection of insiders possible.
- Improved prevention and protection—Advances are needed in a wide range of protection areas, including lower-cost automated monitoring, surveillance, and response; protection from high explosive blasts, projectiles, and fire; interface architectures for CBRNE countermeasures, medical diagnosis, forensic, and detection systems; technology for identification, authentication, and authorization; and personnel surety and determination of intent capabilities.
- Improved large-scale situational awareness and common operating picture—Real-time distributed data collection, fusion, and analysis for large-scale situational awareness of infrastructures is needed. Guidelines must be developed for structure, content, and presentation of the dynamic operational picture.
- Next-generation secure architectures leading to autonomous, self-aware, and self-healing systems—There is a need for the development of technological means for aiding rapid recovery and reconstitution of compromised or damaged systems. New architectures are needed for robust and resilient systems with built-in security. New generations of tools are needed for the design and development of infrastructure components and systems that embody security-oriented principles, methodologies, and techniques, and which produce technology more inherently secure than that available today.



Many of the SSPs will outline additional sector-specific R&D initiatives pertaining to these areas.

#### 6.3.4 Other Department and Agency Infrastructure Protection-Related Plans

Departments and agencies develop emergency response and protective action plans under their own authorities and regulations; the Interim NIPP and the individual SSPs under development should be considered when developing such plans. The responsible planning organization shall coordinate with IAIP, as appropriate, to ensure that these planning efforts are fully informed by the Interim NIPP capabilities and requirements, and updates to the NIPP will address these new plans and programs, where applicable.

## 6.4 International Agreements

In addition to the other plans and programs that the Interim NIPP must coordinate with and support, there is also a set of international agreements designed to collectively contribute to critical infrastructure protection. These include:

- Smart Borders Accord with Canada—This agreement was signed in 2002, and explicitly addresses critical infrastructure protection. It also sets out the U.S.-Canada CIP Framework for Cooperation, which includes several committees looking at a variety of infrastructure protection issues.
- Border Partnership Declaration Accord—This agreement was also signed in 2002; it explicitly addresses critical infrastructure protection. It sets out the U.S.-Mexico CIP Framework for Cooperation, which encompasses six sector-specific working groups.
- U.S.-U.K. Joint Contact Group—This group includes a section for information analysis and infrastructure protection.
- U.S.-Canada S&T CIP Cooperation Agreement—This agreement supports the sharing of science and technology solutions between the U.S. and Canada.

International agreements also include law enforcement-focused arrangements that support CIP, including mutual legal assistance treaties and other international relationships (e.g., the G8 Point of Contact network). Other less-formal arrangements (e.g., resulting from bilateral meetings) exist to forward U.S. infrastructure-protection goals. International outreach has also taken place in such multilateral forums as the U.N. General Assembly, the Asia-Pacific Economic Cooperation, the Organization of American States, and the Organization for Economic Cooperation and Development. All of these efforts have been informed by the National Strategy to Secure Cyberspace and the associated National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, and, most recently, HSPD-7. The Interim NIPP (including the SSPs) will inform future international outreach efforts to reflect priorities identified through DHS's normalization, risk analysis, and prioritization process.

# List of Acronyms

CBRNE	Chemical biological radiological nuclear explosive	NICC	National Infrastructure Coordinating Center
CCV	Characteristics and Common Vulnerabilities	NIMS	National Incident Management System
CIA	Central Intelligence Agency	NIPP	National Infrastructure Protection Plan
CI/KR	Critical infrastructure/key resource	NRP	National Response Plan
CII Act	Critical Infrastructure Information Act of 2002	NSA	National Security Agency
CIP	Critical infrastructure protection	NSSE	National Security Special Event
DHS	U.S. Department of Homeland Security	NSTAC	National Security Telecommunications Advisory Council
EO	Executive Order	ODP	Office for Domestic Preparedness
FBI	Federal Bureau of Investigation	OGC	Office of General Counsel
FOIA	Freedom of Information Act	OMB	Office of Management and Budget
FOUO	For Official Use Only	OSTP	Office of Science and Technology Policy
GCC	Government Coordinating Council	PCII	Protected Critical Infrastructure Information
HSA	Homeland Security Advisor	PMTL	Protective Measures Target List
HSAC	Homeland Security Advisory Council	PRA	Paperwork Reduction Act
HSIN	Homeland Security Information Network	R&D	Research and development
HSOC	Homeland Security Operations Center	SCADA	Supervisory Control and Data Acquisition
HSPD-7	Homeland Security Presidential Directive – 7	S&T	Science and Technology Directorate of DHS
HV/HR	High value/high risk	SCC	Sector Coordinating Council
IA	Information Analysis (Division of DHS IAIP)	SSA	Sector-Specific Agency
IAIP	Information Analysis and Infrastructure Protection Directorate of DHS	SSP	Sector-Specific Plan
IP	Infrastructure Protection (Division of DHS IAIP)	US-CERT	U.S. Computer Emergency Readiness Team
NADB	National Asset Database		
NIAC	National Infrastructure Advisory Council		



Homeland  
Security