



**Homeland
Security**

Guidance for Developing Sector-Specific Plans

As input to the

National Infrastructure Protection Plan

April 2, 2004

For Official Use Only

This page intentionally blank

Table of Contents

	<u>Page</u>
Synopsis	iii
Acronyms	v
1. Background	1
1.1 The National CIP Program	1
1.2 HSPD-7: Identifying, Prioritizing, and Protecting Critical Infrastructure.....	2
1.3 The National Infrastructure Protection Plan	3
1.4 Framework of the NIPP	3
2. Key Terms and Concepts	7
2.1 Critical Infrastructure and Key Resources.....	7
2.2 CI/KR Sectors	8
2.3 Federal Agency Roles and Responsibilities in CIP	13
2.4 Other Key CIP Stakeholders	17
3. National Infrastructure Protection Plan Outline.....	21
4. Sector-Specific Plan Guidance	27
I. Sector Background.....	29
A. Sector Profile.....	29
B. Review of Authorities.....	30
C. Mapping Relationships	31
D. Challenges	33
E. Initiatives	33
F. Milestones	33
II. Identifying Sector Assets.....	35
A. Process for Identifying Sector Assets.....	35
1. Defining Asset Data Parameters	36
2. Collecting Asset Data	37
3. Verifying Asset Data	37
4. Assessing Potential Consequences	38
5. Updating Asset Data	39
B. Challenges	39
C. Initiatives	39
D. Milestones	39
III. Assessing Vulnerabilities and Prioritizing Assets.....	41
A. Process for Assessing Vulnerabilities and Prioritizing Assets.....	41
1. Asset Selection and Description.....	42
2. Analysis of Consequences	42
3. Assessment Methodology	43
4. Prioritizing Assets.....	44
5. Data Issues	45
B. Challenges	46
C. Initiatives	46

D. Milestones	46
IV. Developing Protective Programs.....	47
A. Process for Developing Protective Programs.....	47
B. Challenges	48
C. Initiatives	49
D. Milestones	49
V. Measuring Progress	51
A. CIP Metrics.....	53
1. Core CIP Metrics	53
2. Sector-Specific Goals and Metrics	55
VI. Planning for Research and Development	57
A. Sector Technology Requirements	58
B. Current R&D Initiatives.....	58
C. Gaps.....	58
D. Candidate R&D Initiatives	59
5. Sector-Specific Plan Template.....	61

Synopsis

A fundamental goal of the National Critical Infrastructure Protection (CIP) Program is to identify and protect infrastructures that are deemed most “critical” in terms of national-level public health and safety, governance, economic and national security, and public confidence.¹ The Department of Homeland Security (DHS) recognizes that such protection requires the cooperation and essential collaboration of federal departments and agencies, state and local governments, and the private sector. Accordingly, to achieve the overarching goal of protection, DHS will coordinate the development of consistent, sustainable, effective, and measurable CIP programs across federal, state, and local governments and the private sector.

To guide these efforts, DHS will produce a National Infrastructure Protection Plan (NIPP), a key requirement of Homeland Security Presidential Directive (HSPD) 7. The NIPP design consists of a unifying planning component, including national infrastructure protection goals and performance objectives, a set of individual Sector-Specific Plans, and a national-level cross-sector integration plan. Together, these elements will comprise a comprehensive National Plan for public and private sectors to work together to protect the infrastructure of the United States.

Purpose of this Document

The purpose of this guidance is to provide instructions to Sector-Specific Agencies (SSAs) in drafting their respective plans for implementing CIP responsibilities required under HSPD-7. Although DHS is responsible for the overall National CIP Program, each SSA, because of their expertise, knowledge, and relationships within the sectors, will be responsible for developing a Sector-Specific Plan, which will be incorporated into the NIPP.

The development of the Sector-Specific Plans, and the overall NIPP, will be a dynamic, iterative process. This guidance document provides instructions for the first version of Sector-Specific Plans, which will describe the processes for:

- ❑ Identifying assets within the sector
- ❑ Identifying and assessing vulnerabilities, and prioritizing the assets within the sector
- ❑ Developing sector-specific strategic protective programs
- ❑ Measuring effectiveness of the sector-specific CIP program.

DHS anticipates that these processes will be refined over time as each sector-specific program, as well as the National CIP Program, matures and as lessons learned and best practices are shared among the federal agencies and stakeholders.

How to Use This Document

The guidance is organized into five chapters. Chapters 1, 2, and 3 provide the context and framework and are intended for audiences who may not be familiar with HSPD-7. Chapters 4 and 5 focus specifically on the Sector-Specific Plans.

¹ The term “critical infrastructure,” under the Homeland Security Act, which references the definition in the USA PATRIOT Act, means “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.”

The chapters are as follows:

- ❑ **Chapter 1 – Background:** Provides the context for Sector-Specific Plans, including an overview of the National CIP Program, selected elements of HSPD-7, and the conceptual “framework” for the NIPP.
- ❑ **Chapter 2 – Key Terms and Concepts:** Provides definitions of key terms and concepts used in the National CIP Program.
- ❑ **Chapter 3 – National Infrastructure Protection Plan Outline:** Presents the outline for the overall NIPP, including the Sector-Specific Plans.
- ❑ **Chapter 4 – Sector-Specific Plan Guidance:** Provides detailed instructions for SSAs to use in developing their Sector-Specific Plans. At the beginning of each section of this chapter, the document explains:
 - **Purpose** – What each SSA is expected to provide in that section of the Plan.
 - **Benefits** – Why developing that section of the Plan will help the SSA and DHS in implementing the CIP Program.
 - **Elements** – What sub-sections should be contained within a particular section of the Sector-Specific Plan.
- ❑ **Chapter 5 – Sector-Specific Plan Template:** Provides a plan template on CD-ROM, to assist SSAs in completing and submitting their plans in a consistent format.

Acronyms

BTS	Border and Transportation Security Directorate of DHS
CBP	Customs and Border Protection Bureau
CI/KR	Critical Infrastructure/Key Resource
CII Act	Critical Infrastructure Information Act of 2002
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
DHS	US Department of Homeland Security
DOC	US Department of Commerce
DOD	US Department of Defense
DOE	US Department of Energy
DOI	US Department of the Interior
DOJ	US Department of Justice
DOT	US Department of Transportation
EPA	US Environmental Protection Agency
EP&R	Emergency Preparedness and Response Directorate of DHS
FACA	Federal Advisory Committee Act
FEMA	Federal Emergency Management Agency
FOIA	Freedom of Information Act
GPRA	Government Performance and Results Act
GSA	US General Services Administration
HHS	US Department of Health and Human Services
HSOC	Homeland Security Operations Center
HSPD-7	Homeland Security Presidential Directive - 7
HUD	US Department of Housing and Urban Development
IA	Information Analysis Division of DHS IAIP
IAIP	Information Analysis and Infrastructure Protection Directorate of DHS
ICD	Infrastructure Coordination Division of DHS IAIP
ICE	Immigration and Customs Enforcement Bureau
IP	Infrastructure Protection Division of DHS IAIP
NCS	National Communications System of DHS IAIP
NCSD	National Cyber Security Division of DHS IAIP
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NRC	US Nuclear Regulatory Commission
NRP	National Response Plan
OMB	Office of Management and Budget
OSTP	Office of Science and Technology Policy
PCII	Protected Critical Infrastructure Information
PDD-63	Presidential Decision Directive - 63: Critical Infrastructure Protection
PSD	Protective Security Division of DHS IAIP
PSTN	Public Switched Telecommunications Network
R&D	Research and Development
RMP	Risk Management Program
S&T	Science and Technology Directorate of DHS
SSA	Sector-Specific Agency
SSR	Sector-Specific Responsibility
TSA	Transportation Security Administration
USDA	US Department of Agriculture
USPS	US Postal Service

This page intentionally blank

1. Background

The protection of the nation's critical infrastructure and key resources (CI/KR) is vital to our security, economic vitality, and way of life. The events of September 11, 2001 demonstrated our nation's vulnerability to terrorist attacks. In response to potential threats to our CI/KR, the Information Analysis and Infrastructure Protection (IAIP) Directorate within the Department of Homeland Security (DHS) was established under the Homeland Security Act of 2002, which also established the requirements for the National Critical Infrastructure Protection (CIP) Program.

The vision for the National 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.² In December 2003, the President issued Homeland Security Presidential Directive 7 (HSPD-7) to further direct and strengthen the CIP effort.³

1.1 The National CIP Program

The ultimate goal of the National CIP Program is to protect the nation's critical infrastructure, a responsibility that is shared among the private sector, local and state governments, and the federal government. The Homeland Security Act and the subsequent Presidential strategies on CIP define what must be done to protect the nation's infrastructure.

As shown in Exhibit 1, the National CIP Program is based on a risk-management approach that involves the following key steps:

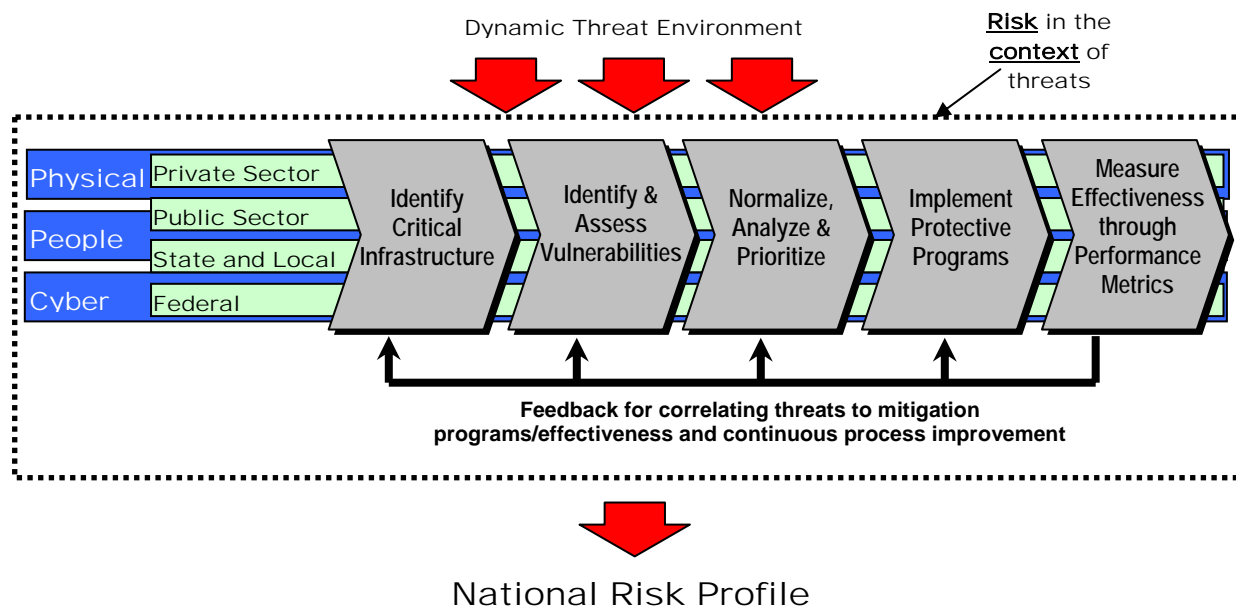
- ❑ **Identifying** the nation's CI/KR and their owner/operators
- ❑ Identifying and assessing the **vulnerabilities** and interdependencies among assets, and analyzing the potential risks to assets based on threats and consequences
- ❑ **Prioritizing** CI/KR based on an analysis and normalization of the risk data (i.e., threats, vulnerability, and consequences)
- ❑ Developing consistent, sustainable, measurable, and effective **programs to protect** CI/KR and implementing those programs when necessary
- ❑ Using **metrics** to measure and communicate program effectiveness.

The last step in this process has two purposes. Overall, performance metrics will be used to constantly improve the alignment of protective programs to the dynamic threat environment, and to drive higher awareness of the threat environment across critical infrastructure owner/operators. This process will provide the information necessary to assist senior officials in making informed decisions about protective actions and national risk management. In addition, metrics will measure program accomplishments and drive continuous improvement of CIP activities.

² "The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets" and "The National Strategy to Secure Cyberspace" (February 2003).

³ 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 1: National CIP Program Implementation



As shown in Exhibit 1, these activities are executed in an integrated fashion across private sector, public sector (e.g., non-governmental, but not privately owned), state and local, and federal infrastructures. Similarly, activities are executed across the physical, people, and cyber components of our CI/KR. The resulting output is the national profile of CI/KR risk, used as the basis for decision-making.

This program is implemented at two levels: in the context of specific threats and in the absence of specific threat information. This two-pronged approach ensures that specific tactical threats are addressed, while allowing the more strategic implementation of protective programs to address future threats.

1.2 HSPD-7: Identifying, Prioritizing, and Protecting Critical Infrastructure

While 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. 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 agencies and departments in working with state and local governments and the private sector to carry out these responsibilities.

HSPD-7 sets several key implementation requirements that are distinct from each other but interrelated:

- ❑ **Integrated National Plan for CI/KR Protection** – Under Paragraph 27, DHS is responsible for developing a National Plan for CI/KR protection, hereinafter referred to as the National Infrastructure Protection Plan (NIPP). The NIPP will include Sector-Specific Plans that address protective activities for the specific CI/KR sectors. The NIPP—and more specifically, the Sector-Specific Plans—is the subject of this guidance.

- ❑ **Annual Plans** – Under Paragraph 35, 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 Sector-Specific Plans.
- ❑ **Internal Federal Plans** – Under Paragraph 24, all federal departments and agencies are responsible for the identification, prioritization, assessment, remediation, and protection of their respective internal CI/KR. The Office of Management and Budget (OMB) is leading the effort to meet this requirement. Under Paragraph 34, federal agencies and departments must submit to OMB these plans for the CI/KR that they own or operate. Plans are due to OMB by July 2004.
- ❑ **Research and Development (R&D) Plan** – Under Paragraph 22, the Office of Science and Technology Policy (OSTP), in coordination with DHS, will coordinate interagency R&D to enhance protection of CI/KR. Under Paragraph 30, DHS, in coordination with OSTP, will prepare an annual federal R&D Plan in support of the directive.

1.3 The National Infrastructure Protection Plan

A key requirement of HSPD-7 is development of the NIPP. The federal government is committed to protecting our nation's CI/KR; this responsibility is shared among the private sector, state and local governments, and the federal government. The NIPP will establish a roadmap and delineate roles and responsibilities for identifying CI/KR, assessing vulnerabilities, prioritizing CI/KR, and determining the protective actions that need to be taken within and across CI/KR sectors. The goal of the NIPP is to ensure an integrated approach to addressing physical, cyber, and human threats and vulnerabilities to consider the full range of risks to the Nation.

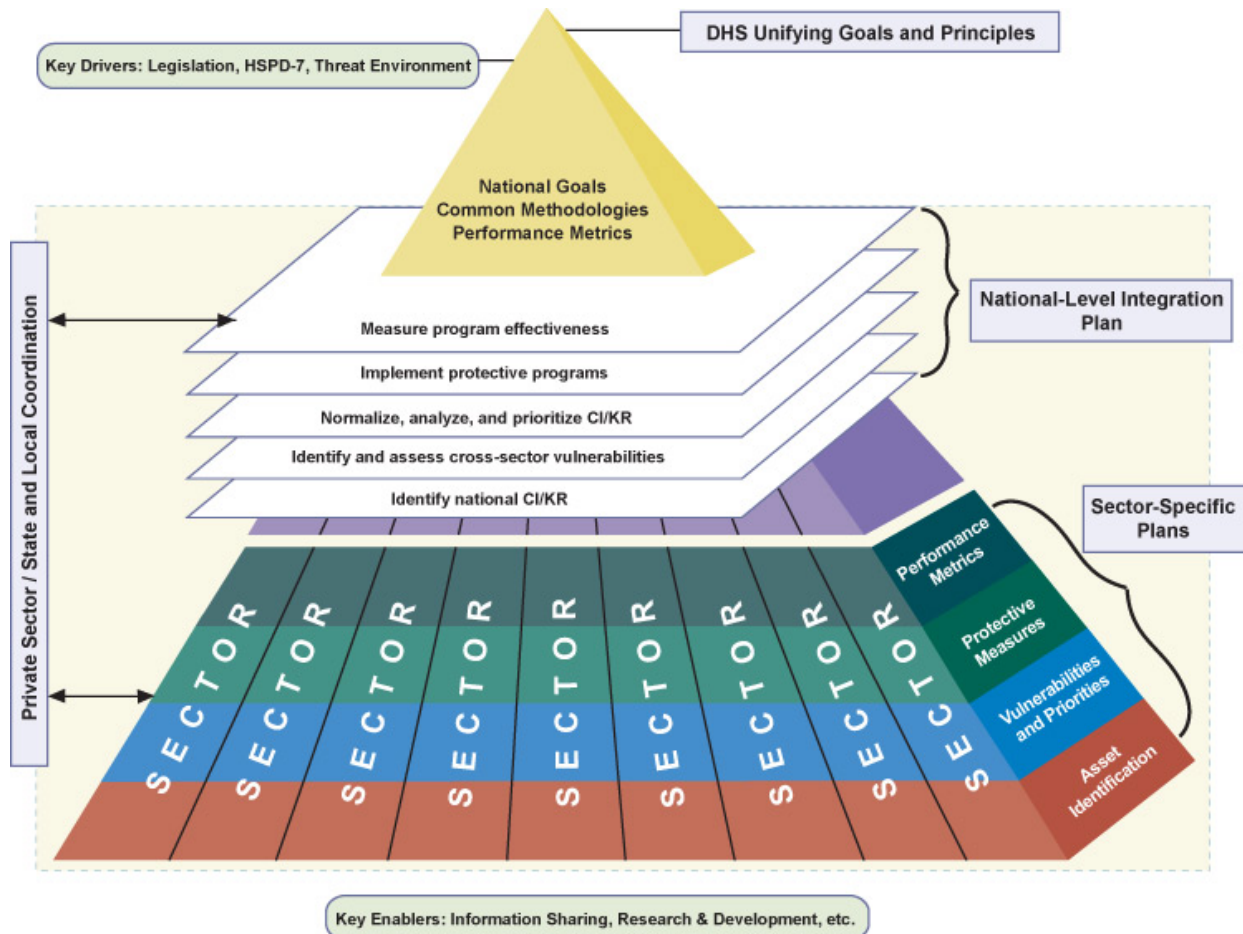
DHS serves as the integrator for this process and provides the single point of accountability and coordination to leverage the sector-specific expertise, relationships, and resources of all stakeholders. The NIPP is intended to provide sector-specific protective strategies and a mechanism for coordinating protective actions across sectors. Through the NIPP, federal, state, local, and private sector stakeholders will implement the National CIP Program in a way that is consistent, sustainable, effective, and measurable.

The NIPP is a member of a family of national plans designed to increase the nation's security through protection, mitigation, response, and recovery. The NIPP will provide the vehicle for assessing vulnerabilities, identifying cross-sector interdependencies, and implementing protective actions. This information can be linked to the operational response mechanisms outlined in the National Response Plan (NRP) and the National Incident Management System (NIMS). The systems and relationships developed through NIPP implementation will be integrated into the response mechanisms identified in the NIMS. That is, when an incident occurs, the "planning information" derived through the NIPP becomes actionable for NRP/NIMS operational information.

1.4 Framework of the NIPP

The conceptual framework for the NIPP is shown in Exhibit 2. As shown in the exhibit, the NIPP will address activities carried out both within individual CI/KR sectors and nationally across sectors, in coordination with private-sector and state and local stakeholders.

Exhibit 2: NIPP Framework



DHS Unifying Goals and Principles. HSPD-7 directs DHS to coordinate the overall national effort to identify, prioritize, and enhance the protection of CI/KR. Thus, as shown at the top of the pyramid in Exhibit 2, DHS will provide the unifying structure and guidance, including the national goals, common methodologies, and performance metrics for the NIPP.

Sector-Specific Plans. At the base of the pyramid in Exhibit 2 are the Sector-Specific Plans. HSPD-7 recognizes that infrastructure sectors have unique characteristics and operating models, and assigns CIP responsibilities for sectors to SSAs, with guidance to be provided by DHS. Under HSPD-7 (Paragraph 19), SSAs are responsible for coordinating protective actions in their designated CI/KR sectors, including conducting or facilitating vulnerability assessments and encouraging protective, risk-management strategies.

To implement these responsibilities, SSAs will develop Sector-Specific Plans that provide an informational foundation for the NIPP. The Sector-Specific Plans will identify the processes by which SSAs conduct the following activities:

- ❑ **Identify assets** within the sector, including owner/operators
- ❑ **Identify and assess vulnerabilities** of these assets to terrorist attack, including determining the potential consequences of such attacks and **prioritizing assets** within a sector, as a starting point for determining where protective actions are needed most
- ❑ **Develop protective programs and measures** based on the detailed knowledge of sector operations
- ❑ **Use metrics** to measure and communicate program effectiveness.

For consistency, SSAs will follow a common outline in developing their Sector-Specific Plans. Detailed instructions for developing the Sector-Specific Plans using the outline are provided in Chapter 4. As provided in Chapter 5, this guidance also includes a CD-ROM template for SSAs to follow in preparing and submitting their plans.

For each of these activities, the SSAs will describe their *approach or methodology* for carrying out the activities. As such, these first iterations of the Sector-Specific Plans are not intended to include the actual data and results of these analyses. The protocols for actually collecting and sharing data on the assets, vulnerabilities, prioritization, and protective strategies are being developed by DHS in collaboration with its stakeholders in state and local governments and the private sector, and will be provided as the basis for future versions of the Sector-Specific Plans.

The Sector-Specific Plans will be reviewed and approved to ensure that the processes outlined for each sector are comprehensive and fundamentally consistent, to allow for national-level and cross-sector analyses. As the methodologies outlined in the Sector-Specific Plans are approved, SSAs will work with DHS to provide access, as needed, to the sector-specific data that will be used by DHS to make national-level infrastructure protection decisions.

However, the protection of the nation's CI/KR cannot wait for the development of a fully refined NIPP and finalized set of Sector-Specific Plans. DHS will use these initial approaches and methodologies provided in the first versions of the Sector-Specific Plans as it continues to implement its risk-based CIP Program in response to the constantly changing threat environment. DHS' ongoing implementation of its National CIP Program in response to specific threat information (i.e., accessing specific CI/KR asset information) will continue to operate during the development and refinement of the Sector-Specific Plans and the NIPP.

National-Level Integration Plan. The middle portion of the pyramid in Exhibit 2 represents the DHS plan for integrating and coordinating CI/KR protective data and activities across sectors and across the nation. This portion of the NIPP will describe:

- ❑ How DHS accesses CI/KR identification data within and across sectors
- ❑ How DHS conducts cross-sector analyses of assets and vulnerabilities to prioritize assets at a national level
- ❑ How DHS uses this information to make immediate protective action decisions (e.g., in the event of a specific threat) or more strategic resource allocation decisions (e.g., where to invest resources for protective actions)
- ❑ How program progress and effectiveness will be measured, assessed, and reported.

Chapter 3 of this guidance presents an annotated outline for the NIPP, to show the relationship between the Sector-Specific Plans and the overall national-level approach.

This page intentionally blank

2. Key Terms and Concepts

This chapter provides definitions and guidance on key terms and concepts used in the National CIP Program and in the NIPP, to ensure that there is consistent understanding of the terms among the SSAs and other stakeholders.

2.1 Critical Infrastructure and Key Resources

Under the Homeland Security Act, which references the definition in the USA PATRIOT Act, the term '**critical infrastructure**' (CI) means "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." The Act defines '**key resources**' (KR) as "publicly or privately controlled resources essential to the minimal operations of the economy and government."

These definitions are broad and must remain so, to provide an appropriate degree of flexibility to the federal agencies and departments, state and local governments, and private sector. This flexibility will enable these stakeholders to use their informed judgment in planning for the protection of critical infrastructure and key resources. To ensure consistency, this guidance provides more detailed descriptions of certain terms to assist SSAs in developing and implementing their plans.

An infrastructure is a collection of assets. As used in this document, an **asset** is something of importance or value, and can include people, property (both tangible and intangible), information, systems, and equipment.⁴ A **system**, which is one type of asset, is a collection of resources or elements made up of any combination of people, physical attributes (e.g., location, structure, etc.), or cyber components that perform a process. Exhibit 3 illustrates these relationships.

Key resources represent individual targets whose destruction could cause large-scale injury, death, or destruction of property and/or profound damage to our national prestige and confidence. Key resources include such facilities as nuclear power plants, dams, government facilities, and commercial facilities. Some key resources, when taken together, may be considered an infrastructure sector.

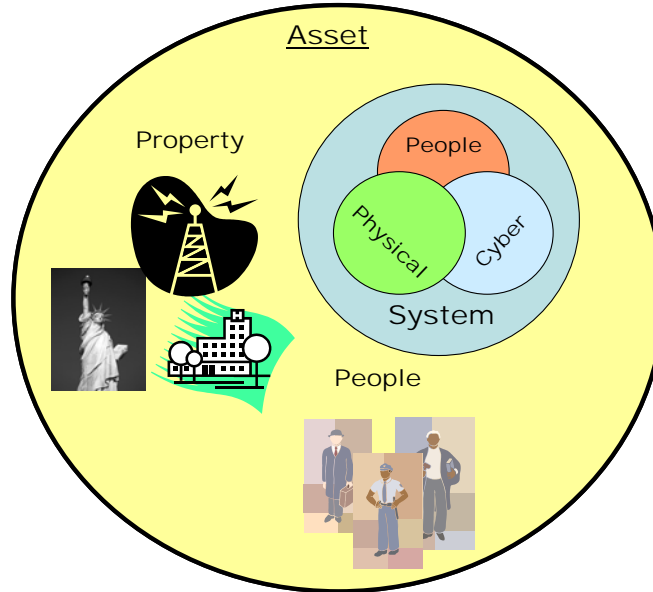
An infrastructure is considered **critical**, or resource is considered **key**, if its destruction or damage causes significant impact on national economic security, public health and safety, psychology and morale, or any combination of these. Chapter 4 of this document provides further guidance on making this determination of criticality when identifying CI/KR. For the purposes of the NIPP, this guidance applies to both critical infrastructure and key resources.

The terms **protect** and **secure**, as defined in HSPD-7, mean "reducing the vulnerability of CI/KR in order to deter, mitigate, or neutralize terrorist attacks." Thus, as used in this guidance, **protection** includes the activities to identify CI/KR, assess vulnerabilities, prioritize CI/KR, and develop protective programs and measures, because these activities ultimately lead to the

⁴ This terminology is consistent with the concept of asset as defined by ASIS International. In its *General Security Risk Assessment Guidelines*, ASIS defines asset as "any real or personal property, tangible or intangible, that a company or individual owns that can be given or assigned a monetary value" and states that "assets include people, all types of property, core business, networks, and information."

implementation of protective strategies to reduce vulnerability. This definition is not intended to expand existing law enforcement activities or other authorities of Sector-Specific Agencies.

Exhibit 3: Assets



Protective actions include detection mechanisms or programs (e.g., surveillance systems that indicate a potential threat), deterrence actions (e.g., enhanced security that reduces the aggressor's likelihood of success and interest in the target), and defensive actions (e.g., physical hardening or buffer zones, to prevent or delay an attack). Protective actions also include actions that reduce the value of an asset (e.g., the incentive to an aggressor to attack) and the effectiveness of such an attack (e.g., creating redundancies in a system and recovery programs that minimize consequences). Strategies for response and recovery also are important.

2.2 CI/KR Sectors

HSPD-7 identified seven SSAs to be responsible for certain unique CI/KR sectors, as follows:

- ❑ **Department of Agriculture (USDA)** – agriculture, food (meat, poultry, egg products)
- ❑ **Department of Health and Human Services (HHS)** – public health, healthcare, and food (other than meat, poultry, egg products)
- ❑ **Environmental Protection Agency (EPA)** – drinking water and water treatment systems
- ❑ **Department of Energy (DOE)** – 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 (Treasury)** – banking and finance
- ❑ **Department of the Interior (DOI)** – national monuments and icons
- ❑ **Department of Defense (DoD)** – defense industrial base

HSPD-7 makes **DHS** responsible for coordinating the protection activities for the following CI/KR: (1) information technology, (2) telecommunications, (3) chemical, (4) transportation systems, (5) emergency services, and (6) postal and shipping. HSPD-7 also indicates that DHS is responsible for coordinating the protection of other key resources, including dams, government facilities, commercial facilities, and nuclear reactors, materials, and waste. Thus, for purposes of the NIPP, DHS will serve as the “SSA” for these 10 CI/KR sectors and resource categories.

The sections below provide brief characterizations of what particular industries, assets, systems, operations, etc., comprise each of the 13 critical infrastructure sectors and four key resource categories identified above. These characterizations generally are based on the descriptions provided in the February 2003 Presidential Strategies.

Agriculture, Food (Meat, Poultry, Egg Products)

The agriculture and food sectors include the supply chains for feed, animals, and animal products; crop production and the supply chains of seed, fertilizer, and other necessary materials; and the post-harvesting components of the food supply chain from processing, production, and packaging through storage and distribution to retail sales, institutional food services, and for restaurant or home consumption. This includes all people, equipment (physical), and cyber components (i.e., plant processing controls) for the sector. Note: For this sector, the food components are limited to meat, poultry, and egg products; other food products are covered by the next sector below.

Public Health, Healthcare, and Food (Other Than Meat, Poultry, Egg Products)

The public health sector consists of state and local health departments, hospitals, health clinics, mental health facilities, nursing homes, blood-supply facilities, laboratories, mortuaries, and pharmaceutical stockpiles. In addition, the industry is founded on the healthcare professional. As technology has advanced, so has the level of integration of cyber within the sector (i.e., electronic record keeping systems). The U.S. also depends on several highly specialized laboratory facilities and assets, especially those related to disease control and vaccine development and storage, such as the Centers for Disease Control and Prevention, the National Institutes of Health, and the National Strategic Stockpile. The food components for this sector are the post-harvesting components of the food supply chain as described in the previous sector, focusing on food other than meat, poultry, and egg products.

Drinking Water and Water Treatment Systems

The water sector consists of two basic, yet vital, components: drinking water supply and wastewater collection and treatment. Although it can be broken down into two basic components, the sector is successful through a complete integration of people, facilities, and cyber-based controls. On the supply side, the primary focus of critical infrastructure protection efforts is the Nation’s 170,000 public water systems. These utilities depend on reservoirs, dams, wells, and aquifers; as well as holding, filtration, cleaning, and treatment facilities, pumping stations, aqueducts, cooling systems, transmission pipelines, and other delivery mechanisms that provide for domestic and industrial applications, including firefighting. The wastewater industry’s emphasis is on the 19,500 municipal sanitary sewer systems, including an estimated 800,000 miles of sewer lines. Wastewater utilities collect and treat sewage and process water from domestic, commercial, and industrial sources. The wastewater sector also includes storm water systems that collect and sometimes treat storm water runoff.

Energy (Including the Production, Refining, Storage, and Distribution of Oil and Gas, and Electric Power Except for Commercial Nuclear Power Facilities)

The energy sector represents a union between cyber control and monitoring systems, physical facilities, and the people that have the sector-specific knowledge base. The energy sector is commonly divided into two segments in the context of critical infrastructure protection: (1) electricity and (2) oil and natural gas. Electric generation assets include fossil fuel plants and hydroelectric dams, transmission and distribution networks linking areas of the national grid, and control and communication systems operating and monitoring critical infrastructure components. Oil and natural gas facilities are widely distributed across the nation, consisting of more than 300,000 producing sites, 4,000 off-shore platforms, more than 600 natural gas processing plants, 153 refineries, and more than 1,400 product terminals and 7,500 bulk stations. The oil infrastructure consists of oil production; crude oil transport; refining and processing; transport, holding, and distribution of refined products and petroleum-derived fuels; and control and other external support systems. The natural gas industry consists of exploration and production, holding, transmission, and local distribution.

Banking and Finance

The banking and financial services sector consists of a variety of physical structures, such as buildings and financial utilities, as well as human capital, operational organizations, and support activities. Physical structures to be protected house retail or wholesale banking operations, financial markets, investment institutions, exchange boards, trading houses, regulatory institutions, and physical repositories for documents and financial assets. Today's financial utilities, such as payment, clearing and settlement systems, are primarily electronic. The financial utilities infrastructure includes such electronic devices as computers, storage devices, and telecommunication networks. In addition, many financial services employees have highly specialized skills and knowledge and are, therefore, considered essential elements of the industry's infrastructure.

National Monuments and Icons

This sector comprises the diverse array of national monuments, symbols, and icons that represent our nation's heritage, traditions, values, and political power. They include a wide variety of sites and structures, such as prominent historical attractions, monuments, cultural icons, and centers of government and commerce. Icons can be considered to include any structure, system, or resource that has cultural, historic, psychological, or political significance at the local, regional, or national-level if compromised or destroyed. As a result, this sector includes many buildings, institutions, and structures (e.g., Golden Gate Bridge, Yankee Stadium, and many local historic buildings) that are not owned or operated by the federal government, which is responsible for most national monuments (e.g., Statue of Liberty, Independence Hall, the Liberty Bell, Mt. Rushmore, and memorials and monuments in Washington, D.C.). While many of these monuments and icons are largely physical in nature, they require people to maintain them and cyber-based systems to enable their maintenance and protection.

Defense Industrial Base

Our nation's defense and military strength rely primarily on the Department of Defense (DoD) and the private sector defense industry that supports it. DoD relies heavily on the private sector to prepare for, plan and execute its core defense missions, including mobilization and

deployment of our nation's military forces abroad. Conversely, private industry and the public at large rely on the federal government to provide for the common defense of our nation and protect our interests both domestically and abroad. Private industry manufactures the majority of the equipment (physical), materials (physical), services, and weaponry (cyber based) used by our armed forces.

Information Technology (IT)

Information Technology encompasses everything from individual computers to vast computing networks that span traditional physical and political boundaries. While many aspects of IT often overlap with the telecommunications sector, it is considered a separate sector because it encompasses more than just communications; that is, IT includes all the hardware and software that makes processing and information sharing possible. Other infrastructure sectors also contain IT resources. Those resources enable functionality of assets within all sectors. Confidentiality, integrity, and availability must be maintained for all IT-based infrastructures in each sector. The SSA for each sector will identify those IT resources. By viewing IT as its own sector, the people, facilities, and cyber-based systems that make IT possible will be assured protection.

Telecommunications

The telecommunications sector provides voice and data service to public and private users through a complex and diverse public-network infrastructure encompassing the Public Switched Telecommunications Network (PSTN), the Internet, and private enterprise networks. The PSTN provides switched circuits for telephone, data, and leased point-to-point services. It consists of physical facilities, including over 20,000 switches, access tandems, and other equipment. These components are connected by nearly two billion miles of fiber and copper cable (physical), dedicated staff to ensuring service (people), and IT systems that monitor and move the data (cyber). The physical PSTN remains the backbone of the infrastructure, with cellular, microwave, and satellite technologies providing extended gateways to the wireless network for mobile users. The Internet consists of a global network of packet-switched networks that use a common set of protocols. Internet Service Providers provide end-users with access to the Internet. Enterprise networks are dedicated networks supporting the voice and data needs and operations of large enterprises. These networks comprise a combination of leased lines or services from the PSTN or Internet providers.

Chemical

The chemical sector is highly diverse in terms of company size and geographic dispersion. Its products and service-delivery systems depend on skilled people, raw materials (physical), manufacturing plants and processes (cyber and physical), and distribution systems (cyber and physical), as well as supporting infrastructure services, such as transportation and electricity products. The chemical sector manufactures products that are fundamental elements of other economic sectors. For example, it produces fertilizer for agriculture, chlorine for water purification, and polymers that create plastics from petroleum for innumerable household and industrial products.

Transportation Systems (Including Mass Transit, Aviation, Maritime, Ground/Surface, and Rail and Pipeline Systems)

The transportation sector consists of physical and cyber-based distribution systems and skilled personnel critical to supporting the national security and economic well being of the nation. Mass transit, which includes rail and bus, carries large numbers of passengers each day, but each city and region has a unique transit system, varying in size and design. The nation's aviation system consists of airports and the associated assets needed to support their operations, including the airlines and aircraft that they serve, and aviation command, control, communications, and information systems needed to support and maintain safe use of our national airspace. The maritime shipping infrastructure includes ports and their associated assets, ships, passenger transportation systems, coastal and inland waterways, locks, dams, canals, and the network of railroads and pipelines that connect these waterborne systems to other transportation networks. Components of the trucking and busing infrastructure include highways, roads, inter-modal terminals, bridges, tunnels, trucks, buses, maintenance facilities, and roadway border crossings. Ground/surface transportation also includes delivery services and personal vehicles. Railroads carry mining, manufacturing, and agricultural products; liquid chemicals and fuels; consumer goods; intercity travelers; and passengers on trains and subways operated by local transit authorities. Several hundred-thousand miles of pipeline span the country and move a variety of substances, including crude oil, refined petroleum products, natural gas, and hazardous materials.

Emergency Services

The emergency services infrastructure consists of fire, rescue, emergency medical services, and law enforcement resources and personnel that are called upon to save lives and property in the event of an accident, natural disaster, or terrorist incident. These services are typically provided at the local level. In addition, state and federal response plans define emergency support functions to assist in the response and recovery. Unlike most critical infrastructures, which are closely tied to specific physical facilities, the emergency services sector consists of highly mobile teams of specialized personnel and equipment (cyber and physical), such as search and rescue teams and metropolitan medical response teams with sophisticated response systems.

Postal and Shipping

This sector includes the U.S. Postal Service plus private carriers such as Fedex and UPS. The vast network operated by the USPS consists of several hundred major processing centers, tens of thousands of delivery and retail units, and hundreds of thousands of official drop-box locations. Transportation assets include delivery vehicle fleets and intra-city trucks. Private carriers own and operate much of their long-distance transportation, and the USPS purchases transportation services. The USPS employs more than 749,000 full-time personnel and touches every residence and business. The USPS alone generates \$60 billion in annual revenues but the importance of the USPS and courriers on the U.S economy is far greater.

Dams

Some of our larger and more symbolic dams are major components of other critical infrastructure systems that provide water and electricity to large populations, cities, and agricultural complexes. There are approximately 80,000 dam facilities identified in the National Inventory of Dams, most of which are small and would not have catastrophic results if they

failed. The federal government is responsible for about 10 percent of the dams whose failure could cause significant property damage or have public health and safety consequences. The remaining facilities belong to state or local governments, utilities, and corporate or private owners.

Government Facilities

Within the overall federal inventory are buildings that the federal government owns and others that it leases from the private sector. The General Services Administration (GSA) is the principal agency responsible for the management of federal government buildings. Additional departments and agencies are similarly involved in the management of federally owned or operated buildings, including DoD and the Department of Veteran Affairs. Most government organizations occupy buildings that are also used by a variety of nongovernmental tenants, such as shops and restaurants. The balance between security and the public's right to access and privacy present challenges in securing these buildings.

Commercial Facilities

Commercial assets include commercial centers, office buildings, sports stadiums, theme parks, and other sites where large numbers of people congregate to pursue business activities, conduct personal commercial transactions, or enjoy recreational pastimes. Day-to-day protection of such facilities is the responsibility of the commercial owners and operators, in cooperation with law enforcement.

Nuclear Reactors, Materials, and Waste

This sector includes the nation's 104 commercial nuclear reactors in 31 states. Nuclear power plants are among the most physically hardened structures within the country, designed to withstand extreme events such as hurricanes, tornadoes, and earthquakes. While losing the capabilities of a single nuclear power plant may have only a minor impact on overall electricity delivery, such a terrorist attack would be considered a significant security event. In an unlikely worst-case scenario, a successful terrorist strike could result in a release of radioactive material. As discussed in Paragraph 29 of HSPD-7, this sector also includes 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.

2.3 Federal Agency Roles and Responsibilities in CIP

The development and implementation of Sector-Specific Plans is a collaborative effort that involves the SSA, as well as other federal agencies and departments, state and local governments, and the private sector. Exhibit 4 indicates which federal agency has the primary role in developing the Sector-Specific Plan and suggests various other federal agencies and departments that may play a supporting role in the development of the Sector-Specific Plans for the 17 CI/KR sectors and categories. However, it must be noted that this guidance does not affect or change existing responsibilities or authorities of federal agencies or departments established by law or policy.

Responsibilities of DHS

As set forth in HSPD-7, DHS is responsible for coordinating the overall national effort to enhance protection of the CI/KR of the United States. DHS is also responsible for establishing uniform policies, approaches, guidelines and methodologies for integrating federal infrastructure protection and risk management activities within and across sectors along with metrics and related criteria for related programs and activities. DHS will oversee development of the NIPP, and will be responsible for approving Sector-Specific Plan approaches and methodologies. This oversight role is shown in Exhibits 4 and 5. In addition, during implementation, DHS will lead, integrate, and coordinate the efforts among federal departments and agencies, state and local governments, and the private sector.

Responsibilities of a Sector-Specific Agency

As set forth in HSPD-7 (Paragraph 6g), “the term ‘Sector-Specific Agency’ means a federal department or agency responsible for infrastructure protection activities in a designated critical infrastructure sector or key resources category. SSAs will conduct their activities under this directive in accordance with guidance provided by DHS.”

To support development of the NIPP, SSAs will be responsible for:

- ❑ Identifying CI/KR in their sector
- ❑ Conducting or facilitating vulnerability assessments for their sector
- ❑ Prioritizing the CI/KR within the sector
- ❑ Developing protective actions for the sector, in cooperation with DHS.

Furthermore, an SSA is responsible for the development, implementation, and maintenance of the Sector-Specific Plan.

The federal agencies that are the SSAs for the 17 sectors are shown in Exhibit 4. This guidance does not change existing responsibilities or authorities of federal agencies or departments. In fact, such authorities can assist in achieving a robust NIPP and in the implementation of the National CIP Program.

Exhibit 5 provides a more detailed breakdown of directorates and divisions within DHS that are responsible for developing the Sector-Specific Plans for those sectors for which DHS is the SSA. These offices are designated in the exhibit as having “Sector-Specific Responsibilities (SSR).” Similar to Exhibit 4, other offices will support these SSR offices in developing the Sector-Specific Plans. Within DHS, IP will provide oversight of plan development, including approval for Sector-Specific Plan approaches and methodologies.

Role of Other Federal Departments and Agencies

Other federal departments and agencies that are not designated as SSAs may nevertheless provide critical support in the protection of a given sector. Specifically, such supporting agencies may participate in development of the Sector-Specific Plan by providing information on aspects or parts of the sector. The supporting agency may also use the SSA as the conduit for sector-related infrastructure information sent to DHS.

Exhibit 4: Federal Agency Responsibilities for Developing Sector-Specific Plans

		DHS	USDA	HHS	EPA	DOE	Treasury	DOI	DOD	DOT	Dept. of State	DOJ	DOC	NRC	OMB	OSTP	HUD	Dept. of Education	USPS
Critical Infrastructure Sectors		SSAs								Other Federal Agencies									
	Agriculture, Food (Meat, Poultry, Egg Products)	O	SSA		S						S		S			S		S	
	Public Health, Healthcare, Food (Other than Meat, Poultry and Egg Products)	O		SSA	S						S					S			
	Drinking Water and Water Treatment Systems	O		S	SSA			S			S					S			
	Energy (Except Commercial Nuclear Power Facilities)	O				SSA		S		S	S					S			
	Banking and Finance	O					SSA				S		S			S	S		
	National Monuments and Icons	O						SSA	S		S					S			
	Defense Industrial Base	O							SSA		S					S			
	Information Technology	SSA									S	S	S		S	S			
	Telecommunications	SSA									S		S			S			
	Chemical	SSA			S						S		S			S			
	Transportation Systems	SSA								S	S					S			
	Emergency Services	SSA		S	S	S			S		S	S				S			
	Postal and Shipping	SSA								S	S					S			S
Key Resources	Dams	SSA						S	S		S					S			
	Government Facilities	SSA	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
	Commercial Facilities	SSA									S		S			S			
	Nuclear Reactors, Materials, and Waste	SSA				S					S			S		S			
SSA	Sector-Specific Agency	Note: This exhibit is non-exhaustive and only provides suggestions of agencies that may play a supporting role in developing a Sector-Specific Plan. SSAs are responsible for identifying and coordinating with the appropriate stakeholders in the federal and state and local government, and the private sector for plan development. DHS will provide an oversight and approval function for SSA plan development.																	
S	Supporting																		
O	Oversight																		

Exhibit 5: Internal DHS Responsibilities for Developing Sector-Specific Plans

		IP	HSOC	IA	TSA	ICE	CBP	FEMA	S&T	US Secret Service	US Coast Guard	Chief Info Officer
		IAIP			BTS			EP&R	S&T	Secretary		
Critical Infrastructure Sectors	Agriculture & Food (Meat, Poultry, Egg Products)	O					S		S			
	Public Health, Healthcare, Food (Other than Meat, Poultry & Egg Products)	O				S			S			
	Drinking Water/Water Treatment	O							S			
	Energy (Except Nuclear Power Facilities)	O			S				S			
	Banking and Finance	O							S	S		
	National Monuments and Icons	O							S			
	Defense Industrial Base	O							S		S	
	Information Technology	SSR							S	S		
	Telecommunications	SSR	S						S			
	Chemical	SSR			S				S			
	Transportation Systems	O			SSR	S	S		S		S	
	Emergency Services	O	S	S	S			SSR	S	S	S	
	Postal & Shipping	O			SSR	S	S		S			
Key Resources	Dams	SSR						S	S			
	Government Facilities	O				S		SSR	S			S
	Commercial Facilities	SSR							S			
	Nuclear Reactors, Materials, & Waste	SSR							S			
	SSR	Sector Specific Responsibility										
	S	Supporting										
	O	Oversight										

For example, although DHS is the SSA for the chemical sector, it recognizes that EPA, as the primary regulatory agency for chemical facilities, will play a significant role in developing the Sector-Specific Plan for the chemical sector. Similarly, since both the Energy and Transportation sectors cover pipelines for oil transport, it is expected that DOE and DHS will work together to sort out responsibilities for these assets in their respective sectors. However, if necessary, DHS will adjudicate issues regarding such shared responsibilities when an asset or system crosses sectors.

Exhibit 4 indicates some of the agencies that are anticipated to provide support for developing Sector-Specific Plans for various sectors. These agencies are designated in Exhibit 4 as “S.” This list of supporting agencies is not exhaustive and should be considered a starting point for discussion. As discussed in Chapter 4, it is the responsibility of SSAs to identify the appropriate agencies that will be involved in development of the Sector-Specific Plans.

2.4 Other Key CIP Stakeholders

Each SSA has mutually beneficial relationships with and an understanding of its private sector constituents, its state and local agencies, and other key stakeholders. The SSAs are responsible for ensuring that these stakeholders are appropriately involved in the development of the Sector-Specific Plan, as some (e.g., private sector owners and operators of CI/KR) will play a key role in plan implementation.

State and Local Agencies

Engagement with state and local authorities, including tribal authorities, is an important part of protecting the many CI/KR sectors. State and local governments play a critical role in planning and implementing detection, prevention, and mitigation programs within the communities where CI/KR reside. They often constitute the front line of defense in support of the security spectrum, and act as conduits for requests for federal assistance when the threat exceeds local and private sector capabilities. States also are involved in identifying CI/KR and assessing vulnerabilities. For example, under a DHS grant program in the Office for Domestic Preparedness, states conduct vulnerability, risk, and needs assessments, and develop and implement statewide homeland security strategies. Furthermore, the Homeland Security Advisor in each state serves as the principal point of contact for DHS on homeland security issues. For certain CI/KR, state and local agencies may serve as owner/operators for a significant portion of the sector.

There are organizations at the state and local levels with long histories and well-established networks in dealing with disaster response requirements, law enforcement issues and public welfare concerns. Since September 11, 2001 many of these organizations have increased their focus on areas of public awareness, preparedness, and protection. The Sector-Specific Plans must have a mechanism for identifying state and local organizations that have capabilities that will be beneficial in the implementation of the NIPP. It is the intent of the NIPP effort to fully engage state and local stakeholders as an avenue for approaching and coordinating with asset owner/operators in protection of their assets.

Private Sector

Private industry owns and operates an estimated 85 percent of the nation’s CI/KR. Partnering with them in the planning process is crucial for successful implementation. Customarily, 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. In implementing the NIPP, it is likely that the private sector owners and operators of the CI/KR will assess their vulnerabilities and implement protective programs with guidance from SSAs, DHS, and other Homeland Security implementation partners, such as state and local governments.

Private industry has long been organizing itself to promote industry best practices and to influence regulatory aspects of specific industries to promote the development and protection of industry interests. Industry reaction to September 11, 2001 galvanized many industry associations and major institutions to provide additional focus on the protection of industry assets against potential loss from terrorist attacks. In the Sector-Specific Plans, SSAs must identify a mechanism for outreach to appropriate industry forums. The majority of protective actions will be taken by the asset owners. The lessons learned and best practices that have evolved over the years of corporate collaboration are vital to the successful protection of the nation's critical infrastructures. This plan envisions that formal mechanisms will be established for industry input to the NIPP process.

Information Sharing and Analysis Centers (ISACs)

ISACs have been established in many of the infrastructure sectors. These organizations are mostly private sector industry-based. They were established to share information and analysis in specific sectors for alerts, warnings, and advisories. ISACs represent another example of the commitment of private sector industries to strengthening the security of their assets. As part of the overall NIPP approach, DHS will provide guidance to all SSAs for the development of ISACs. The IAIP Infrastructure Coordination Division is tasked with the development of programmatic ISAC policy and implementation. In addition to their relationship with SSAs, ISACs will have direct information sharing relationships and operational communication with IAIP. As part of this effort, SSAs will identify, in their Sector-Specific Plans, currently operating ISACs and similar organizations, and recommend approaches for integrating these organizations into the overall NIPP.

Sector Leadership

As a point of entry into the sector, "Sector Leadership," referred to by HSPD-7 as a "sector coordination mechanism," refers to the infrastructure sector individual, entity, or group recognized by the SSA as representing the sector. This designation should occur as a result of joint SSA and DHS discussions with the private sector entities of their infrastructure sector, and should not function in any manner that would violate provisions of the Federal Advisory Committee Act (FACA). Responsibilities of Sector Leadership may include:

- ❑ Coordinating the development of sector-wide input into the NIPP, in partnership with the SSA.
- ❑ Leading outreach and awareness programs to support infrastructure protection plan implementation.
- ❑ Leading the vulnerability assessments of the sector to cyber, physical, or personnel attacks, and recommending actions to reduce and eliminate significant vulnerabilities.
- ❑ Leading the development of requirements for, and leading the oversight of sector ISAC effectiveness, tailored to the special needs of the sector and supportive of its infrastructure protection programs.

- ❑ Reviewing sector-wide guidelines, standards, and effective practices on infrastructure protection, identifying and developing needed sector-wide training, education, and implementation metrics for success in infrastructure protection activities.
- ❑ Assessing requirements for research and development necessary to meet the special needs of the sector.
- ❑ Serving as the coordination point for the sector's owners and operators in discussions with other sectors as needed (identify interdependencies, address common issues, share effective practices and lessons learned).
- ❑ Acting as the point of contact for the sector with the federal government at infrastructure protection meetings, and serving as the strategic communication point back into the sector and its members from the federal government.
- ❑ Identifying and communicating obstacles or impediments to an effective infrastructure protection program.

This page intentionally blank

3. National Infrastructure Protection Plan Outline

This chapter presents the overall outline for the NIPP, including the Sector-Specific Plans, so that SSAs can see where their plans will fit in the overall plan structure. To ensure national consistency across sectors, each SSA will be expected to follow the Sector-Specific Plan outline in developing their plans.

Exhibit 6 below presents the NIPP outline. This is followed by a more detailed, annotated outline of the main body of the NIPP to provide further reference. Chapter 4 provides specific guidance and instructions for developing each component of the Sector-Specific Plan portion of the NIPP outline. Chapter 5 of this guidance provides the CD-ROM template for Sector-Specific Plans.

Exhibit 6: NIPP Outline

I. Background and Purpose

- A. Background and Objectives of the National CIP Program
- B. Purpose of the NIPP

II. Strategy

- A. Concept of Operations for the National CIP Program
- B. Scope of the NIPP
- C. Roles and Relationships in National CIP Program Implementation

III. Actions

- A. Identify CI/KR
- B. Identify and Assess Vulnerabilities
- C. Analyze, Normalize, and Prioritize CI/KR
- D. Develop and Implement Protective Programs for CI/KR
- E. Measure Effectiveness
- F. Research and Development

IV. Information Sharing

V. Implementation

- A. Key Milestones
- B. Integration with Other Plans

Appendices: Sector-Specific Plans

Each Sector-Specific Plan is organized as follows:

- I. Sector Background
- II. Identifying Sector Assets
- III. Assessing Vulnerabilities and Prioritizing Assets
- IV. Developing Protective Programs
- V. Measuring Progress
- VI. Planning for Research and Development

Annotated Outline for the NIPP

I. Background and Purpose

A. Background and Objectives of the National CIP Program

This section will provide background on the National CIP Program, and describe the overall objectives – what the Program is trying to achieve and what it will look like when the objectives are accomplished.

B. Purpose of the NIPP

This section will explain the purpose of the NIPP, which is to provide the mechanism for establishing a dynamic, integrated National Critical CIP Program that reduces the vulnerability of CI/KR to terrorist attacks through:

- ❑ Identification of CI/KR assets
- ❑ Assessment and prioritization of CI/KR vulnerabilities
- ❑ Development and implementation of protection programs
- ❑ Sharing of CI/KR information.

II. Strategy

A. Concept of Operations for the National CIP Program

This section of the NIPP will describe the framework for how the National CIP Program is organized and operates at two levels:

- ❑ **Strategic** – DHS and SSAs work with their stakeholders to identify CI/KR, assess vulnerabilities, prioritize CI/KR, and establish protective action programs based on general threat information for each sector. DHS uses this information to create a comprehensive national picture of CI/KR and vulnerabilities and to implement prioritized protective action programs based on this information across all sectors.
- ❑ **Tactical** – The strategic National CIP Program is implemented in the context of specific threat information. DHS reexamines previous work on assessed vulnerabilities and established protective action programs in light of the specific threat information. Actual threat warnings are then issued and certain protective actions are recommended/taken.

B. Scope of the NIPP

This section of the NIPP will describe what CI/KR sectors are addressed in the Plan and which federal agencies are involved.

C. Roles and Relationships in National CIP Program Implementation

This section of the NIPP will describe the roles and responsibilities of all stakeholders in the implementation of the National CIP Program.

1. DHS responsibilities – Examples include:

- ✓ Developing and operating the integrated National CIP Program through coordination with stakeholders
- ✓ Obtaining access to CI/KR data across sectors

- ✓ Conducting vulnerability assessments within and across sectors, analyzing interdependencies, and prioritizing CI/KR nationally
- ✓ Identifying and implementing protective strategies where appropriate;
- ✓ Coordinating and communicating with the private sector
- ✓ Measuring and communicating program effectiveness.

2. SSA Responsibilities – Examples Include:

- ✓ Communicating and collaborating with private-sector asset owner/operators and other stakeholders (sector-organizing)
- ✓ Working with their stakeholders to identify CI/KR, assess vulnerability, prioritize assets, and develop protective programs
- ✓ Providing subject matter and industry specific expertise.

3. State and Local Agency Responsibilities – Examples Include:

- ✓ Assisting in the identification of CI/KR and assessment of vulnerabilities, including coordinating with asset owner/operators
- ✓ Planning and implementing detection, prevention, and mitigation programs within their communities
- ✓ Facilitating the involvement of state and local organizations that can contribute to implementation of the NIPP.

4. Private-Sector Responsibilities – Examples Include:

- ✓ Assessing vulnerabilities and implementing protective programs for their assets and industries
- ✓ Exchanging information with SSAs, DHS, and other partners on lessons learned and best practices in protecting their assets and industries
- ✓ Being represented on ISACs for information sharing and analysis in specific-sectors for alerts, warnings, and advisories.

5. Other Federal Agency Responsibilities – Examples Include:

- ✓ Supporting SSAs and DHS by leveraging their mandates, subject matter knowledge, and relationships
- ✓ Coordinating on how cross-sector CI/KR is effectively addressed
- ✓ Making sector-specific information available to SSAs and DHS.

III. Actions

A. Identify CI/KR

This section will describe the methodology by which DHS will access multiple virtual databases to assimilate and integrate CI/KR information across sectors (based on input from the SSAs) to develop a comprehensive national picture of CI/KR. DHS will validate CI/KR inventories and will provide a process for continuous updating of CI/KR identification and assessment.

B. Identify and Assess Vulnerabilities

In this section, DHS will describe the process by which it will share generalized threat information with SSAs to allow them to conduct initial vulnerability assessments within their sector. DHS will also describe how it assists various sectors in determining the

appropriate criteria, developing vulnerability assessment tools, and performing some vulnerability assessments at specific sites.

C. Analyze, Normalize, and Prioritize CI/KR

This section describes methodology for analyzing vulnerabilities, threats, and consequences to determine overall risks across CI/KR. A key “value-added” step is DHS’ interdependency analysis of vulnerability across all sectors. This cross-sector analysis will provide the comprehensive national picture of CI/KR and vulnerabilities needed to ensure protection. Following this, DHS will normalize the data to allow a comparison of vulnerabilities and risk across the sectors. DHS will use this information to determine how and when to implement protective strategies and as a guide for research needs and priorities.

D. Develop and Implement Protective Programs for CI/KR

This section will describe how DHS will use information provided by SSAs to analyze existing protective programs, and to identify and share best practices with SSAs, state and local governments, and the private sector. DHS will describe a process for working with the SSAs in an ongoing reassessment of the effectiveness of protective programs to identify best practices and common shortfalls across sectors. In addition, DHS will describe the process for working with the private sector to develop and implement protective actions for specific CI/KR.

E. Measure Effectiveness

This section of the NIPP will describe how DHS will use performance metrics to determine the effectiveness of the National CIP Program. Performance metrics are indicators of the degree to which a program is accomplishing its goals. Activities (e.g., vulnerability assessments of water facilities) can be measured by process metrics (e.g., the number of assessments performed by a certain date) and by outcome metrics (e.g., a reduced number of facilities assessed as high risk, following the institution of protective actions.) The National CIP Program will be measured using both process and outcome metrics. Selecting outcome metrics for protection programs is challenging because risk reduction is not directly observable (i.e., it is difficult to determine whether a terrorist attack has been prevented). Nonetheless, process metrics alone are not sufficient to measure the value of CIP activities. Some SSAs are successfully using outcome metrics to improve their CIP programs. DHS intends to identify those best practices and translate them to other sectors as appropriate.

F. Research and Development

The DHS Science and Technology (S&T) Directorate is leading the development of the first annual Federal CIP R&D Plan. They are coordinating with the Infrastructure Subcommittee of the National Science and Technology Council of OSTP. The Subcommittee has physical and cyber security subgroups that are together forming an integrated R&D Plan. They are engaging all federal agencies and departments to identify R&D initiatives with potential CIP applications. They will engage SSAs to identify CIP requirements that could be fulfilled by technology.

This NIPP guidance does not generate an R&D planning requirement separate from the effort being led by DHS S&T. Instead, for the NIPP, each SSA will import a sector-specific R&D summary based on the Federal CIP R&D Plan. The SSA will develop this

summary supported by S&T and based on the R&D Plan. IAIP will develop the cross-sector R&D summary supported by S&T and based on the R&D Plan.

IV. Information Sharing

This section will summarize both DHS and SSA relationships to the private sector and initiatives for sharing CIP information among all stakeholders. Information sharing includes sharing information on the identification of CI/KR and protecting it, best practices for vulnerability assessments and protective actions, and threat warning data (from DHS to stakeholders).

V. Implementation

A. Key Milestones

This section of the NIPP will provide specific timeframes by which key programs and activities (e.g., implementation of Sector-Specific Plans) are to be accomplished. It will include discussion of the Annual Sector plan updates.

B. Integration with Other Plans

This section of the NIPP will describe how the Plan relates to 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.

This page intentionally blank

4. Sector-Specific Plan Guidance

This chapter presents instructions to SSAs in developing their Sector-Specific Plans, following the plan outline presented in the previous chapter. In the next chapter, a template is provided to assist SSAs in completing their plans.

This page intentionally blank

I. Sector Background

This chapter provides instructions for developing Part I of the Sector-Specific Plan, on Sector Background.

Purpose: In this part of the Plan, SSAs will characterize their sector, describe the context in which the SSA interacts with the stakeholders, and identify authorities and regulations relevant to protective activities.

Benefits: This information will ensure that the readers of a Sector-Specific Plan understand the nature and complexity of the sector and the current relationships among stakeholders. DHS will use this information to understand how the SSA views its sector responsibilities; to obtain information on the key stakeholders in the sector and how they relate to each other; and to determine legal authorities for implementing the program.

Elements:

- I. Sector Background
 - A. Sector Profile
 - B. Review of Authorities
 - C. Mapping Relationships
 - D. Challenges
 - E. Initiatives
 - F. Milestones

Given the diverse nature of CI/KR, it is important to ensure that readers of the NIPP understand the nature and complexity of each CI/KR sector, including the current roles, responsibilities, and relationships among the various stakeholders. This section of the Sector-Specific Plan will provide a “snapshot” of the sector and describe how involved the various stakeholders are in conducting protective activities.

A. Sector Profile

As a first step in designing the approach to implementing HSPD-7, SSAs should characterize their sectors. It is important to understand how each SSA views the boundaries and characteristics of its sector assets, to ensure that any potential gaps, as well as any overlaps in scope between sectors are identified and addressed.

Section 2.2 of this document provided basic descriptions of each sector. Using these descriptions as a starting point, SSAs should provide a full characterization of the CI/KR assets that are covered in their sector. Where appropriate, SSAs should describe the sector in terms of sub-categorizations or classes of assets, particularly if the sector includes obviously distinct types of operations, businesses, facilities, etc. For example, at the highest level, the transportation sector will be divided into transportation modes (e.g., air, rail, highway, marine, etc).

The characterization may also include a description of the entities that own or operate the various assets or classes of assets (e.g., owners who are private industry versus municipalities).

B. Review of Authorities

As part of the sector background, the SSA will prepare information on governing authorities (e.g., laws, rules, regulations, orders, etc.) applicable to the protection of assets within the sector. This includes any authorities pertinent to:

- ❑ Collection of asset-specific information (e.g., can a permitting authority be used to collect pertinent information relevant to the structure or operation of a particular facility?)
- ❑ Information sharing and protection
- ❑ Conducting vulnerability assessments (e.g., for some sectors, vulnerability assessments are already required under other statutes, such as the Bioterrorism Act)
- ❑ Identifying protective strategies
- ❑ Implementing protective programs.

This information will be valuable as a tool to demonstrate actions already underway, to determine impediments to implementing HSPD-7, and to provide opportunities to increase protective programs through utilizing existing authorities. This information is to include pertinent sections of authorities that could specifically relate to asset protection, even if those authorities have current application in other areas. An example of such a review follows as Exhibit 7, using the Chemical Sector. This example is provided for illustrative purposes and should not be considered complete.

Exhibit 7: Example of a Partial Review of Authorities for the Chemical Sector

For this sector, authorities have been included that address security, safety, and other areas applicable to the continued and safe operation of the sector infrastructure.

Authorities of SSA

- ❑ Under HSPD-7, DHS is assigned responsibility as the Sector-Specific Agency to protect the chemical sector.
- ❑ Under the Homeland Security Act of 2002, DHS has responsibility to analyze critical infrastructure vulnerability, including those in the chemical sector. Also under the Act, DHS issued an interim rule on Procedures for Handling Critical Infrastructure Information, which provides protection of critical infrastructure information submitted to DHS by the private sector.
- ❑ Congress authorized funding of DHS for completing vulnerability assessments at chemical facilities.
- ❑ Legislation is now pending that will mandate chemical facilities to implement security measures to protect against terrorist attacks.

Authorities of DHS (if not SSA)

- ❑ See above

Authorities of Other Departments and Agencies

- ❑ Under the Clean Air Act Section 112(r), the U.S. Environmental Protection Agency (EPA) has issued Risk Management Program (RMP) regulations that require certain chemical facilities to develop RMP plans to prevent chemical accidents.
- ❑ The Chemical Safety Information, Site Security, and Fuels Regulatory Relief Act limits public access to RMP off-site consequence information out of concern for terrorism. DOJ/EPA jointly issued these regulations.
- ❑ Under the Emergency Planning and Community Right-to-Know Act, the U.S. EPA issued regulations that require state/local governments and chemical facilities to be involved in emergency response planning for and notification of chemical accidents.

Note: Key state and local authorities also should be captured. In some instances, there also may be applicable international law (e.g., transportation).

In addition to identifying authorities that exist, the SSA should also identify the gaps in authority that could hinder the CIP process. The SSA may also list other guidance or policy documents that guide the regulation and oversight of sector activities.

C. Mapping Relationships

A fully engaged sector will involve the participation of individual private sector businesses, trade organizations and associations, state/local/tribal authorities, and other stakeholders who represent the full breadth and depth of the sector. The effective engagement of sector stakeholders by SSAs must utilize relationships and activities that are proven to be effective, and also employ new approaches to streamline and expedite action. The status of the SSA's current relationships within the sector will be useful in identifying successful efforts, in recognizing the complexity and diversity of sectors that require active subcomponents, and in targeting areas where further outreach is desired and assistance from DHS may be helpful.

Sections 2.3 and 2.4 of this guidance provided general descriptions of the various roles and responsibilities of other federal agencies, asset owner/operators, private-sector coordination groups, and state and local agencies. In this section of the Sector-Specific Plan, SSAs should describe their understanding of sector roles and responsibilities for the following entities: (1) private sector organizations (including asset owner/operators); (2) other federal departments and agencies (including DHS); and (3) state and local agencies. As indicated below, SSAs need to discuss the strategy for interacting with these entities and the current relationships with them.

Relationships with Private Sector Owner/Operators and Organizations

It has been estimated that private industry owns or operates about 85 percent of the nation's CI/KR, so these owners/operators will have a large role in identifying CI/KR and implementing protective programs. In this section, the SSA should describe its existing relationships with asset owner/operators and other private sector organizations, as well as general expectations for how these stakeholders will support the development and implementation of the Sector-Specific Plan. Sample questions to address include:

- ❑ What mechanisms are in place within the SSA to ensure regular interaction with the sector?
- ❑ What parts of the SSA organization have liaison functions with the sector?
- ❑ How does the SSA leverage activities to grow participation in and bring breadth and depth to sector organizations?
- ❑ How will the SSA reach other potential sector members?
- ❑ What strategies and approaches are in place to continually engage with existing sector participants?
- ❑ What strategies and approaches are underway to increase the participation of the sector?
- ❑ What forums or communication vehicles provide for information sharing?
- ❑ What protocols exist, informally and formally, regarding information sharing with the sector?
- ❑ Are there different processes for sharing threat/warning data?

- ❑ How many institutions make up the sector? How many of these institutions directly participate in information sharing through the ISAC?
- ❑ How often and in what manner does interaction occur?
- ❑ What strategies, activities, and approaches has the ISAC delivered to date?
- ❑ What is the relationship between the ISAC and Sector Leadership coordinating mechanisms? How are their roles and responsibilities delineated?
- ❑ What parts of the sector are missing from this group?
- ❑ What strategies, activities, and approaches has the Sector Leadership delivered to date?

Relationships with Other Federal Departments and Agencies

As discussed in Section 2.3 of this guidance, other federal departments and agencies may play a supporting role in protecting the sector. In this section, the SSA should identify the agencies and departments that will provide such a supporting role and describe the SSA's relationship to those agencies.

A starting point for developing this section is to review Exhibit 4 presented in Section 2.3 of this guidance document. As an example, EPA supports the Agriculture, Public Health, Chemical, Emergency Services, and the Government Facility sectors through its regulatory responsibilities and agency mission; similarly, the Department of Commerce supports the Agriculture, Banking and Finance, Information Technology, Telecommunications, Chemical, Government Facilities, and Commercial Facilities sectors. In this section, the SSA should describe its current relationships with these agencies, as well as expectations for their roles and responsibilities in developing and implementing the Sector-Specific Plan. Sample questions to address include:

- ❑ What agencies play support roles to the SSA's sector?
- ❑ What efforts does the SSA undertake to include and leverage support agency relationships with the sector?
- ❑ How do supporting agencies implement aspects of the Plan on behalf of the SSA in all of, or in parts of, the sector?
- ❑ How are supporting agencies providing information on aspects or parts of the sector for the SSA to integrate into an overall sector view (e.g., for the annual Sector-Specific Report)?
- ❑ How do the supporting agencies use the SSA as the conduit for sector-related infrastructure information sent to IAIP (or at a minimum, include the SSA in such communications)?

Furthermore, DHS (particularly within the IAIP Directorate) contains several divisions that regularly engage with the private sector, while other divisions are involved in protective strategy activities and emergency response. In this section, the SSA should also explain its relationship to DHS. Some questions to address include:

- ❑ How does the SSA interact with DHS?
- ❑ Which DHS offices are critical to sector relationships?

Relationships with State and Local Agencies

In many cases, state and local agencies serve as the front line for interface with sector owners and operators of CI/KR. Some sector examples include public health, drinking water and water treatment, transportation systems, emergency services, dams, and government facilities. Their planning processes, data collection activities, governing and regulatory authorities, and responsibilities regarding public safety and emergency response, will provide key information and resources to SSA efforts. In this section, the SSA should describe its relationships with these state and local agencies, and expectations for their roles in supporting the development and implementation of the Sector-Specific Plan. Some questions to address include:

- ❑ How does the SSA involve state and local governments?
- ❑ How are impediments in reaching the appropriate state and local players overcome?
- ❑ What organizations representing state and local governments are being utilized?
- ❑ How often and in what manner does interaction occur?

D. Challenges

The SSA should identify any challenges to working or communicating with its stakeholders as well as identify conflicting regulatory authorities or significant regulatory gaps, if any.

E. Initiatives

In this section of the Sector-Specific Plan, SSAs should indicate recent or current activities with respect to sector relationships that demonstrate success and that can be useful models for other sectors. SSAs should also identify future planned initiatives or strategies. Some sample questions include:

- ❑ What organizational components of the sector operate as an effective means of regular information sharing and relationship building?
- ❑ What specific actions or methodologies have been developed within the sector that would be valuable and applicable to other sectors?
- ❑ What future initiatives for building sector relationships are being planned or developed?

F. Milestones

If there are any planned initiatives to expand sector relationships, these should be indicated along with responsibilities and dates for each initiative.

This page intentionally blank

II. Identifying Sector Assets

This section provides instructions for completing Part II of the Sector-Specific Plans on Identifying Sector Assets. Identifying assets is the first step in the CIP Program implementation process, as shown in the illustration below.



Purpose: The purpose of this part of the Plan is for the SSA to explain the process that it will use to gather information on those sector assets that could potentially be critical (i.e., those that, if damaged, result in significant consequences – impacts on national economic security, national public health, safety, psychology, or some combination of these).

Benefit: This data gathering and analysis will provide the SSA and DHS with a comprehensive inventory of assets, which can then be further analyzed with respect to vulnerabilities and protective actions.

Elements:

- II. Identifying Sector Assets
 - A. Process for Identifying Sector Assets
 - 1. Defining Asset Data Parameters
 - 2. Collecting Asset Data
 - 3. Verifying Asset Data
 - 4. Assessing Potential Consequences
 - 5. Updating Asset Data
 - B. Challenges
 - C. Initiatives
 - D. Milestones

A. Process for Identifying Sector Assets

One of the key areas to be addressed in each Sector-Specific Plan is the methodology for identifying and maintaining current data on CI/KR. While CI/KR are predominantly owned and operated by the private sector, each SSA must first develop an inventory of its sector assets. The resulting inventory will be used by the SSA to coordinate protective actions within the sector, as well as by DHS, which requires a national picture of all CI/KR assets to coordinate national protective programs.

The initial collection of data on potential CI/KR assets in each sector is intentionally broad and comprehensive, as it is the first step in a series of analyses that will sequentially reduce the universe of assets to those that appear to be most critical and require the greatest focus of resources and protective actions. However, the starting point for this analysis should not include every individual component of the sector systems (e.g., all telephone poles or all transformers), rather those assets or systems that are large enough to be considered targets for attack and that may potentially be candidates for protective actions. Assets of interest are those with the potential to cause national impacts, not every component of the infrastructure.

It may be helpful to identify asset classes or categories, rather than discrete assets in some cases. Examples include aircraft or vessels of a certain size or type, types of financial institutions, or groups of individuals, such as maintenance personnel. Such categories may support the identification of assets that are more people-oriented or intangible in nature (e.g., the airspace in a region). In some cases, more intangible assets can be linked with one or more physical or cyber assets in the same system (e.g., regional airspace with the regional control system).

1. Defining Asset Data Parameters

As a first step in identifying assets across the sector, the SSA must first define the specific information that it will collect about each asset. This definition of what data are needed will be used to provide instructions to the private sector, which for most sectors, will be the source of the information. This step will narrow the scope of the data received to avoid delivery of an overabundance of information.

In identifying assets, SSAs must ensure that they take a comprehensive, integrated view of the asset to include all of its characteristics and dependencies for it to function. Many assets are dependent on multiple elements and systems to maintain functionality (i.e., people, physical, information technology, telecommunications, etc.). Asset elements as well as asset interdependencies will be taken into consideration when developing protective strategies and determining vulnerabilities. Additional guidance addressing this issue is provided in subsequent sections.

The following list suggests minimum categories of information to be collected for each asset. SSAs may include additional categories of information to better characterize sector assets as needed. The basic parameters the SSA requires for the given sector should be specified to ensure consistency in data collection across the sector, along with the basis for their selection.

General information to be gathered for each asset (where applicable):

- ☐ Asset name and address or general description of location (e.g., meat processing facility ABC, XYZ Inc., etc.)
- ☐ Owner/operator name and address (e.g., ABC Company, contact person, address, telephone number, etc.)
- ☐ Sector (e.g., transportation, energy, etc.)
- ☐ Asset class or sub-sector (e.g., transportation-marine, etc.)
- ☐ Region/service area (e.g., Midwest, Northeast, etc.)
- ☐ Tracking/identification number (if applicable)
- ☐ Seasonality/frequency of use
- ☐ Function within the infrastructure (e.g., XYZ Inc. makes batteries for missiles).

Other information for each asset (as available):

- ☐ System components that are central to the mission and function (names of major systems)
- ☐ Dependencies (e.g., what does the asset depend on to function?)
- ☐ Interdependencies (e.g., what depends on it: people, physical, information technology, telecommunications, economics, other sectors, etc.?)
- ☐ Continuity and redundancy to include back-ups built into the asset

- ❑ Impact on sector in cases of loss or failure (e.g., economic, public health and welfare, public psyche, national security)
- ❑ Existing protective actions (e.g., fencing, biometrics, firewalls, etc.).

2. Collecting Asset Data

The next step is to identify and describe how the SSA will collect or obtain access to this information, currently and in the future (as the information will constantly change). At a minimum, the description of this data collection process must include:

- ❑ Description of how the SSA will reach out to the entire sector (e.g., who will be contacted and why? How will the SSA know whether the inventory covers the appropriate universe of assets?)
- ❑ Description of how data will be provided to the SSA (e.g., format of data, means of communicating data)
- ❑ Timeframe for providing the data
- ❑ Data consolidation process
- ❑ Privacy of data.

Components of an efficient data collection process should include leveraging existing outreach mechanisms and groups familiar to the private sector. Many private-sector constituents already have established contacts, interaction, and dialogue opportunities with each agency through various mechanisms. Use these types of existing communication channels when possible. These channels may include ISACs, agency task forces, public sector summits, voluntary and public/private partnerships. Other outreach channels include industry and membership associations, chambers of commerce, and agency regional offices. Alternatively, a joint planning process may be initiated for data collection in which DHS and SSA meet with sector owner/operators.

SSAs should be aware that the asset data may qualify for one or more exemptions from public disclosure under the Freedom of Information Act (FOIA). SSAs should consult with the FOIA Officers and/or Offices of General Counsel of their respective agencies to obtain specific guidance on the possible protections from public disclosure by one of the exemptions or special exclusions.

Also, SSAs must be aware, and must advise their private sector constituents, that at this time the PCII Interim Rule does not afford protection to voluntarily submitted critical infrastructure information that is submitted to any SSA other than DHS. Should private sector entities wish to submit information under the auspices of the CII Act of 2002 and the PCII Interim Rule, they should be referred to the PCII Program web site at www.dhs.gov/pcii for specific details on how to properly submit the information to the PCII Program Office at DHS.

3. Verifying Asset Data

Once the asset data has been received by the SSA, it must be verified. In this section of the Plan, the SSA will describe the process for ensuring that information collected is reliable. The process for verifying data for assets must include the following:

- ❑ Protocol for reviewing data (e.g., sample size, criteria, frequency)
- ❑ Steps to address incomplete and/or inaccurate data

- ❑ Follow-up activities required based on the infrastructure's significance (e.g., onsite meetings, validation of owner/operator procedures, etc.).

4. Assessing Potential Consequences

Once the asset data has been gathered, SSAs must establish a process to provide an initial assessment of the potential consequences that may result if the asset were compromised. The intent of this analysis is to provide a first screen of the assets within a sector to determine which are potentially most critical to national security and which might be candidates for protective actions. This allows further evaluations such as vulnerability assessments to be focused where they may be most beneficial, given resource constraints both within government agencies (federal, state, and local) and among private sector organizations.

This analysis will be based on the inherent characteristics of the asset or system, and identifying the “worst-case” consequences that would result if the asset were destroyed, disrupted, or exploited. As set forth in HSPD-7, the focus should be on the potential for situations that could:⁵

- ❑ Cause catastrophic health effects or mass casualties, comparable to those from the use of a weapon of mass destruction
- ❑ Impair federal agencies' abilities to perform essential missions, or ensure public health and safety
- ❑ Undermine state and local 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 methodology for assessing consequence should include a system for “scoring” each asset against a potential consequence. The purpose of the scoring system is to discriminate among and stratify the assets according to the scale of potential consequences. Consequences may be expressed in terms of standard service parameters (e.g., loss of electricity to 50,000 properties for 2 days) or in terms of the ultimate outcomes, such as economic loss, numbers of deaths, etc. The Sector-Specific Plan should describe how impacts to other sectors also are identified and considered.

For purposes of tracking performance metrics, discussed in Section V of this Sector-Specific Plan, the scoring approach should include at least three different ranking categories for each type of consequence, with a minimum threshold below which consequences are not considered to be significant. Representative examples of these scoring categories include:

- ❑ Population affected: level 1: 100 to 1,000 casualties; level 2: 1,000 to 10,000 casualties; level 3: greater than 10,000 casualties
- ❑ Economic consequences: level 1: \$300 million to \$3 billion; level 2: \$3 billion to \$30 billion; level 3: greater than \$30 billion

⁵ Paragraph (7), sections (a) through (f) of HSPD-7.

- ❑ Impacts on national morale: level 1: destruction of one national icon; level 2: destruction of several icons; level 3: destruction of more than several icons.

Note that these examples are for illustrative purposes only – scoring systems developed for each sector should address the full range of potential consequences outlined above.

Once the assets have been analyzed against the scoring criteria, the assets should be placed in the appropriate group, based on the highest level of consequence they are associated with for any of the consequence types. For example, if an asset scores high on only one criterion, but lower on all the rest, it should still be placed in the “level 3” group. The assets with potential consequences in the highest two ranges for one or more of the consequence types will be of greatest concern for subsequent analyses and will be the focus of the performance metrics.

5. Updating Asset Data

Asset data from the sector must be routinely updated and made available, so that both the SSA and DHS will be able to leverage the most up-to-date data when making decisions concerning national protection strategies. This section of the plan must describe the SSAs process for ensuring access to continuously updated asset data for the sector. The process should include the following:

- ❑ Frequency of updates (e.g., as changes occur and/or on a routine basis)
- ❑ How updated information will be provided
- ❑ Considerations for reevaluation of the sector inventory itself
- ❑ SSA division/office that will be responsible for obtaining the data
- ❑ Security clearance level of the data
- ❑ How the SSA will notify DHS of data updates.

B. Challenges

Challenges that must be overcome within each sector with regard to identifying assets, should also be described (e.g., collecting and maintaining potentially sensitive data or sharing best practices) along with the proposed approach to dealing with them. DHS will review this information to identify crosscutting or common challenges that would benefit from an integrated solution.

C. Initiatives

In this section, the SSA should describe the status of initiatives that are underway or planned for developing or enhancing the process of identifying critical assets, including the development of key elements of the Plan that are not currently available.

D. Milestones

The SSA should indicate milestones for the initiatives and other efforts described in the previous section. Responsibilities and dates must be given for each milestone. Target goals for implementing the various processes (e.g., all assets identified by April 2005) should be listed if they have already been established by the SSA.

This page intentionally blank

III. Assessing Vulnerabilities and Prioritizing Assets

This section of the guidance provides instructions for developing Part III of the Sector-Specific Plans on Assessing Vulnerabilities and Prioritizing Assets. These activities comprise the second and third steps, respectively, in the CIP Program implementation process. Normalizing, analyzing, and prioritizing have a more essential role at the national level than at the sector level. Within the sectors, this step is more directly tied to the output of the vulnerability assessments and has been described as such.



Purpose: The purpose of this part of the Plan is for each SSA to describe its current approaches for identifying and assessing vulnerabilities of assets in its sector, and to describe how this information will be provided to and/or shared with DHS on an ongoing basis. It also includes the SSA's approach to prioritizing assets based on the results of the vulnerability assessments.

Benefits: The evaluation of vulnerabilities and prioritizing of assets will allow the SSA and asset owner/operators to understand where protective strategies are needed due to the potential for significant consequences and vulnerabilities. DHS will use this information to select those assets across all sectors that warrant the most attention in terms of protective strategies as well as to help determine research needs and priorities. The intelligence community typically looks at places and regions more than assets – therefore, some of the prioritization that is ultimately done at the national level may take different slices through the “data” set.

Elements:

III. Assessing Vulnerabilities and Prioritizing Assets

- A. Process for Assessing Vulnerabilities and Prioritizing Assets
 - 1. Asset Selection and Description
 - 2. Analysis of Consequences
 - 3. Assessment Methodology
 - 4. Prioritizing Assets
 - 5. Data Issues
- B. Challenges
- C. Initiatives
- D. Milestones

A. Process for Assessing Vulnerabilities and Prioritizing Assets

Vulnerability can be described as characteristics of a physical infrastructure's design or operation/use that render assets susceptible to damage, destruction, or incapacitation by one or more types of hazard, including terrorist acts, mechanical failures, and natural hazards. For the human and cyber elements of a system, vulnerabilities may present themselves 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 as well as those that may cause failure due to inadvertent human actions or natural disasters.

The remainder of this guidance focuses on security-related vulnerabilities that could be intentionally exploited, as these are the ones most likely to have national-level effects. However, SSAs are cautioned to be mindful of all vulnerabilities when suggesting protective strategies (see Section IV of this Sector-Specific Plan), as multi-use solutions are often the most cost-effective, most likely to be sustained over time as threat perceptions fade, and most likely to be undertaken voluntarily by asset owner/operators.

A **vulnerability assessment** is a systematic process in which a CI/KR system is reviewed to identify areas of weakness (as well as the potential actions that would exploit those weaknesses) and determine the effectiveness of additional security measures, alone or in combination. Throughout this section, the term “vulnerability assessment” is used to represent a process, not a specific vulnerability assessment tool. Different levels of detail might be appropriate for each category of prioritized assets.

An effective assessment of vulnerabilities serves as the foundation of a prioritized plan for security upgrades, modifications of operational procedures, and/or policy changes to reduce the risks and vulnerabilities to critical assets. The assessment process provides a framework for developing risk reduction options and associated costs.

1. Asset Selection and Description

Vulnerability assessments can be conducted at many different levels of detail, and can focus on an asset, a set of interdependent assets, an asset class or sub-sector, or a sector. The SSA has the responsibility of ensuring that all the necessary vulnerability assessments are conducted within the sector—whether the assessments are conducted at the sector or sub-sector level by the SSA or are self-assessments carried out by the asset owner/operators or others (such as a state agency). Each SSA must determine whether it is more appropriate and beneficial to roll-up individual asset assessments or to conduct one or more higher-level assessments of the entire sector or sub-sectors. Depending on the perceived significance of a particular asset, DHS may work in partnership with the SSA or its constituents on a particular vulnerability assessment or may conduct an independent assessment, if the sector's timetable does not meet DHS' needs.

In this section of the Sector-Specific Plan, the SSA should describe how the vulnerability assessment will be applied (e.g., whether the SSA will analyze assets individually or by some grouping, such as asset classes or sub-sectors).

2. Analysis of Consequences

The vulnerability assessment starts by determining the consequences of concern. As discussed in the previous section, these consequences include:

- ❑ Health or safety impacts – catastrophic health effects or mass casualties
- ❑ Impacts on national security and function – impacts on governmental ability to perform essential missions, ensure public health and safety, maintain order, or deliver essential public services

- ❑ Economic impacts – impact on private sector’s capability to ensure the orderly functioning of the economy and delivery of essential services; impact on the economy through the cascading disruption of other CI/KR
- ❑ Psychological impacts – impacts on the public’s morale and confidence in our national economic and political institutions.

In the previous section, an evaluation was conducted to determine the broad range of all possible and worst-case outcomes from an event. In this section, these consequences are analyzed further to determine those that would be expected to occur from specific causal actions.

As part of this analysis, the SSA may determine that the focus should be on particular types of consequences (e.g., catastrophic health effects rather than financial implications), because, for the specific assets involved, one type of consequence may dominate. For example, an attack on a chemical plant may have minor impact on the national economy, but may have catastrophic acute and chronic health effects on the local population.

The purpose of this step is to ensure that the vulnerability assessment process (described below) focuses on the true potential for consequences and leads to an estimate of risk. As part of this process, the SSA should revisit the categories of consequence (associated with the asset identification step) to ensure that they adequately reflect the range of actual impacts and can discriminate among assets. For example, this analysis may conclude that a previously defined level 3 for population affected (e.g., greater than 10,000 casualties) may not be possible, given the specific assets. As a result, the levels for population affected may need to be readjusted into tighter bins.

3. Assessment Methodology

In this section, the SSA should provide a description of the methodology(ies) used to assess vulnerabilities within the sector. The purpose of the vulnerability assessment is to identify the potential weaknesses that could result in the consequences of concern.

As described above, vulnerabilities should be defined as the intrinsic weaknesses in the asset, as well as the causal action that would exploit these weaknesses. Such causal actions will include potential terrorist actions (e.g., use of explosives, biological agents, cyber disruption, etc). In this process, SSAs should assume that all terrorist-related hazards are credible and have equal probability of occurrence – that is, they should focus on the vulnerability to all known threats or threat classes without consideration of the likelihood of a given event at the time of the assessment. In contrast, at the national level, DHS will apply specific threat information to the sector-specific vulnerability assessments, both within and across sectors, to prioritize the needs for specific protective actions.

The purpose of this section is for the SSA to describe how the methodology will rank the vulnerabilities to demonstrate the likelihood that the vulnerability can be successfully exploited (independent of the probability of an attack). 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. Similar to consequences, vulnerabilities should be categorized into 3 to 5 “bins” (e.g., low, medium, and high).

In describing the assessment methodology, the SSA should also address the following issues:

- ❑ Is one methodology used for all asset classes, or are different approaches taken to address the different characteristics of assets within one sector?
- ❑ What is the basis of the methodology? For example, is it dictated by sector-specific regulations (federal, state, or local) or best practices and industry standards?
- ❑ How are vulnerabilities assessed for each of the specific elements within an asset (i.e., the cyber, human, and physical elements)?
- ❑ How does the methodology address protective programs already in place, such as mechanisms or systems for detection, delay, and response; cyber protection features; or existing security policies and procedures?
- ❑ How does the methodology address interdependencies, such as consequences on other sectors, and single points of failure for multiple assets in the sector?
- ❑ Does the vulnerability assessment consider consequences resulting from attacks on nearby structures or systems, rather than on the asset itself?
- ❑ How does the methodology incorporate known vulnerabilities that may have been identified in other studies or assessments for similar sites, as well as those determined for other sectors where there is also applicability to the sector of concern?

The description of the methodology should also address how the methodology is implemented. Examples of issues to address include:

- ❑ What type and quality of information is used (e.g., expert judgment, versus modeling of consequences, field observations, desktop reviews, aggregate data for groups of assets)?
- ❑ Are there standards for those individuals who conduct assessments, including third party assessors?
- ❑ How will the SSA verify all or some self-assessments, if self-assessments are anticipated?
- ❑ How often are assessments conducted and what are the triggers for (unscheduled) assessment updates?

4. Prioritizing Assets

In this section, the SSA will describe its approach for prioritizing the sector's assets based on risk, to determine which would benefit most from protective strategies. In this analysis, overall risk is determined based on a combination of vulnerabilities, consequences, interdependencies, and the general threat environment (i.e., assuming equal probability that all vulnerabilities will be exploited).

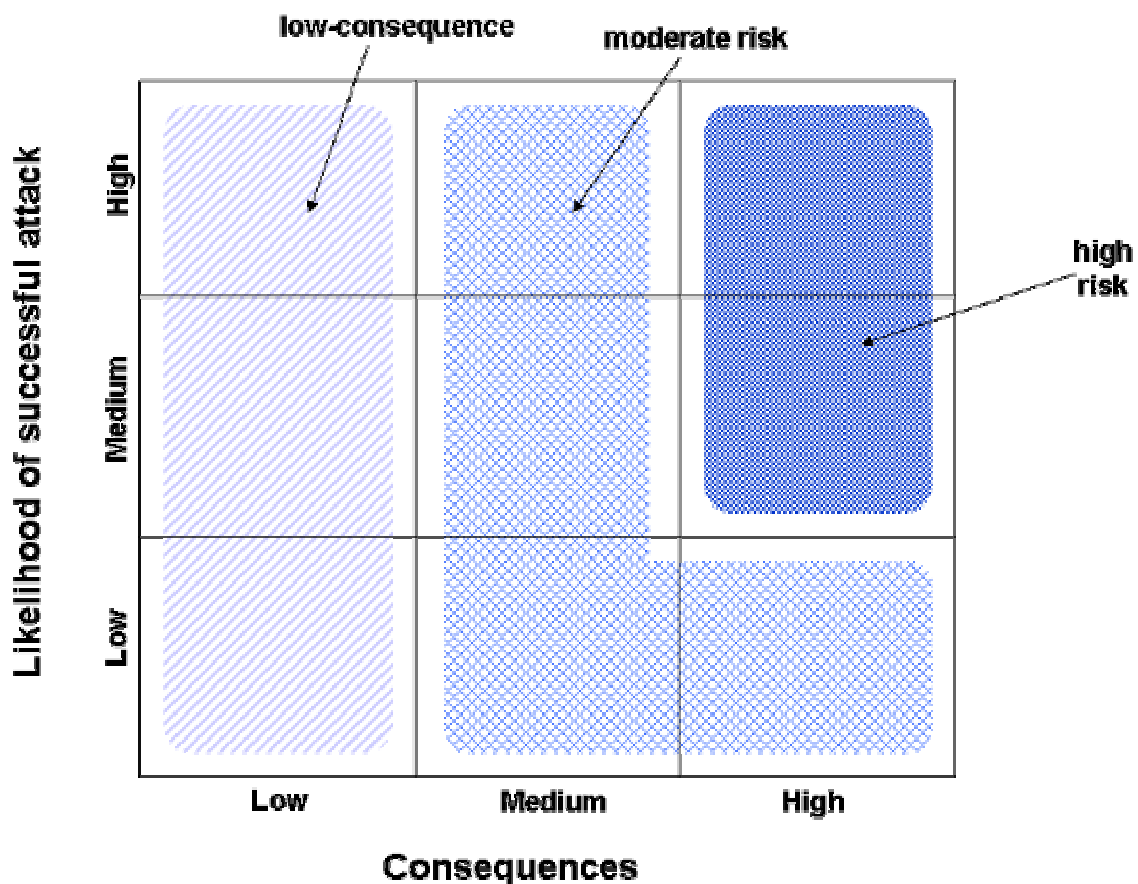
A systematic and consistent way of prioritizing assets offers transparency and increases the defensibility of the decisions that are made about resource allocation. It also reduces the focus on individual companies or assets and helps to determine what is of national importance in terms of potential impact.

The methodology described in the Plan should first describe how the SSA scored consequences and vulnerabilities, as discussed above (e.g., the SSA has defined

consequences as level 1, 2, and 3, and has defined vulnerabilities as low, medium, and high). Next, the methodology should describe how these scores will then be rolled up for the various event scenarios considered for each asset, to create an overall risk score. As discussed previously, the purpose of a scoring system is to discriminate among and stratify the assets. Although it is not necessary or desirable to provide a strict rank ordering of assets based on risk (e.g., 1 to 100), it is desirable to have 3 to 5 categories or “bins” of risk (e.g., very-low, low, medium, medium-high, and high).

To identify the risk level of assets, the SSA could use a risk matrix with likelihood of success of an attack on one axis and potential consequences on the other axis, as illustrated in Exhibit 8. High-risk assets would be those with a high score for potential consequences and at least a moderate likelihood of attack success.

Exhibit 8: Sample Risk Matrix



As part of the description, the SSA should describe who will carry out the prioritization and whether it will be conducted independently of the vulnerability assessment, or whether the criteria are sufficiently defined, such that the ultimate priority can be included in the vulnerability assessment process.

5. Data Issues

In this section, the SSA should describe the processes for obtaining and ensuring access to data on vulnerability assessments and the results of prioritization efforts. This should include

where and how the information will be maintained, how DHS may access information on specific assets when needed, and how confidential or sensitive information will be handled. A process for applying the lessons learned from one asset to other assets without revealing confidential or sensitive information should also be described.

The Plan should also describe how updated information on vulnerabilities and sector priorities will be obtained. This should include specifying how the SSA will be informed if significant changes in protective programs are made at one or more assets that change the vulnerability assessment and priority, as well as how the SSA will then share that information with DHS.

B. Challenges

Challenges that must be overcome within each sector with regard to assessing vulnerabilities and prioritizing assets should be described (e.g., collecting and maintaining potentially sensitive data, sharing best practices, or developing a prioritization process that differentiates between various national icons), along with the proposed approach to dealing with them. DHS will review this information to identify crosscutting or common challenges that would benefit from a more integrated solution.

C. Initiatives

In this section, the SSA should describe the status of initiatives that are underway or planned to develop or enhance the processes for assessing vulnerabilities and prioritizing assets, including the development of key elements of the Plan that are not currently available.

D. Milestones

The SSA should indicate milestones for the initiatives and other efforts described in the previous section. Responsibilities and dates must be given for each milestone. Target goals for implementing the various processes should be listed if they have already been established by the SSA.

IV. Developing Protective Programs

This section provides instructions for completing Part IV of the Sector-Specific Plans on Developing Protective Programs. This process of developing protective programs based on the SSA's knowledge of sector operations is the fourth step in the CIP Program implementation process, as shown in the graphic below.



Purpose: In this part of the Plan, the SSA will explain how it will work with the sector stakeholders to develop one or more sector-specific programs to protect its high-risk assets.

Benefits: Protective programs guide asset owners/operators on the most effective strategies given the general classes of threats that are applicable to that sector and the vulnerabilities common to the assets in the sector.

Elements:

- IV. Developing Protective Programs
 - A. Process for Developing Protective Programs
 - B. Challenges
 - C. Initiatives
 - D. Milestones

A. Process for Developing 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. Each sector needs a tailored strategy and programs to best protect the unique assets within the sector. Because of the highly distributed and massive nature of infrastructure sectors, the responsibility for protecting assets must be shared among the SSA, the state and local government, and private sector, in coordination with DHS.

Given the SSAs' understanding of the activities, operations, and assets in their sectors, they can provide an informed perspective on the most effective long-term protective strategies. The SSAs will also be in the position to review the vulnerability assessments across their sector for best practices and shared needs across multiple assets.

In this section of the Sector-Specific Plan, the SSA should describe how it will work with the sector stakeholders to develop sector-specific programs that will provide effective long-term protection of the sector's CI/KR. This description should include the following elements:

- ❑ Roles and responsibilities of sector stakeholders
- ❑ How critical information generated from plan implementation, particularly the information on which assets appear to pose the highest risk, will be considered

- ❑ How stakeholders will share best practices for long-term protective programs, including overcoming implementation challenges
- ❑ How often and by which entity the protective programs will be updated and refined.

Particular attention should be paid in the process to identifying the appropriate roles of the sector stakeholders. The role of some stakeholders (e.g., federal agency) may be to create the atmosphere or encourage the implementation of protective programs. Other stakeholders will ultimately take actions for implementing the protective programs. The roles should reflect existing authorities (e.g., regulatory) and relationships of the sector stakeholders.

The protective program should, at a minimum, ensure that it covers those assets that appear to have the highest risk. General approaches for protecting assets include:

- ❑ **Prevent or Delay an incident** – enhanced police presence, restricting access, fencing, structural integrity, vehicle checkpoints, and cyber protection features such as additional access controls. Within the sector, such measures are generally taken by the asset owner/operators, and may vary by threat level.
- ❑ **Detect a potential incident** – intrusion detection systems, monitoring, operation alarms, and employee security awareness programs. These actions are also taken at the asset level and are generally permanent changes.
- ❑ **Mitigate or respond to an incident** – adequate response plans can mitigate impacts and potentially enable the sector asset to resume operations sooner. Such plans may involve multiple stakeholders within the sector, including state and local agencies.
- ❑ **Recover from an incident** – continuity of operations plans. These plans may be asset-specific or it may be developed for a set of assets.

Both mitigation and recovery can benefit from additional redundancy at either an asset or sub-sector level.

In protective programs, there also may be shared protective actions for many of the sector stakeholders, such as developing a protocol to protect sensitive information among stakeholders.

Protective programs should address separately actions for tactical response (e.g., ISAC threat information needing action within hours or days) versus more long-term strategic response. DHS will play the lead role in developing tactical measures for the most critical assets in response to specific threats. The sector stakeholders will address more long-term strategies (e.g., redundancy) as well as tactical responses for other assets and for those measures within the control of the asset owner/operator.

B. Challenges

Challenges that must be overcome within each sector with regard to developing protective programs should also be described (e.g., sharing best practices), along with the proposed approach to dealing with them. DHS will review this information to identify crosscutting or common challenges that would benefit from a more integrated solution.

C. Initiatives

In the last part of this section, the SSA should describe the status of initiatives that are underway or planned for developing or enhancing the process for developing protective programs, including the development of key elements of the Plan that are not currently available.

D. Milestones

The SSA should indicate milestones for the initiatives and other efforts described in the previous section. Responsibilities and dates must be given for each milestone. Target goals for implementing the various processes should be listed if they have already been established by the SSA.

This page intentionally blank

V. Measuring Progress

This section provides instructions for completing Part V of the Sector-Specific Plans on Measuring Progress. Tracking program performance and progress is the last step in the CIP Program implementation process, as shown in the graphic below.



Purpose: This part of the Plan explains how SSAs will design and implement performance metrics for implementation of Sector-Specific Plans.

Benefits: An effective measurement system clarifies program goals, since performance metrics relate to goals. Measurement quantifies the benefits achieved by CIP activities, and supports feedback to improve program activities and better allocate resources.

Elements:

V. Measuring Progress

A. CIP Metrics

1. Core Metrics
2. Sector-Specific Goals and Metrics

Overview of Metrics and CIP Goals

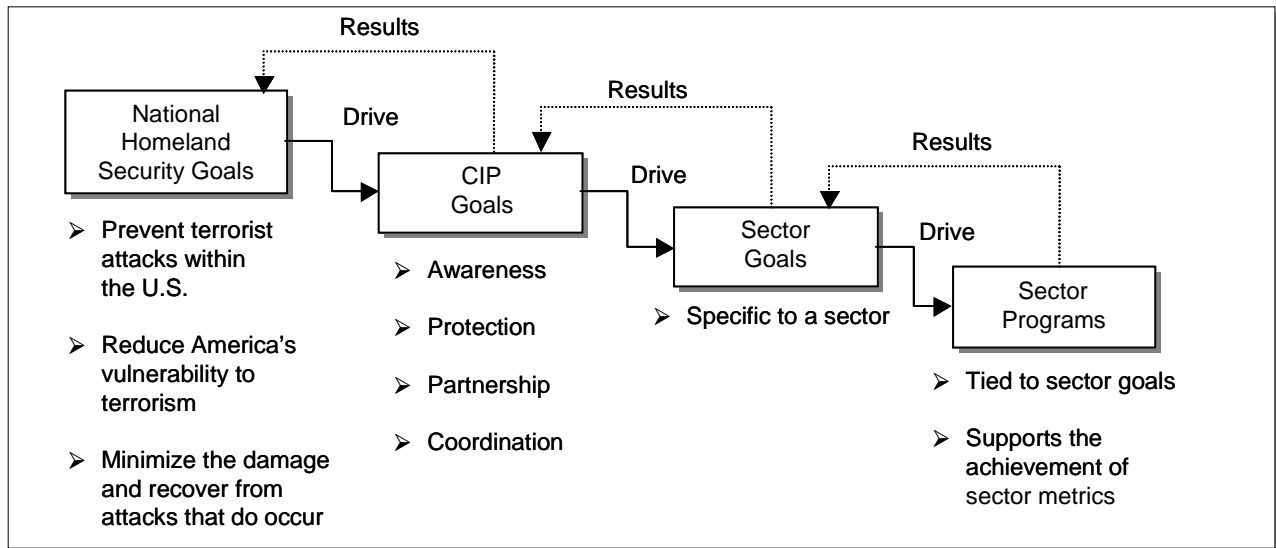
The CIP Program will use a metrics-based system of performance evaluation, in conformity with the Government Performance and Results Act (GPRA).⁶ Metrics provide a basis for establishing accountability, documenting actual performance, facilitating diagnoses, and promoting effective management. Metrics supply the data to affirm that specific goals are being met, or to show what corrective actions may be required to stay on target.

In this part of the Plan, SSAs should describe their performance measurement program. This program will consist of measuring performance against several core metrics common to all sectors, as well as sector-specific metrics.

Before establishing an effective metrics program, it is important to understand the overall goals and strategies to be achieved. In particular, national Homeland Security goals drive National CIP Program goals, which then drive sector-specific program goals. Exhibit 9 illustrates this hierarchy of goals.

⁶ This guidance intends to match OMB performance measurement requirements. OMB offers performance measurement guidance and examples for performance metrics in Circular A-11, part 6, "Preparation and Submission of Strategic Plans, Annual Performance Plans, and Annual Program Performance Reports." NIST offers performance measurement guidance for cyber security through Special Publication 800-55, "Security Metrics Guide for Information Technology Systems."

Exhibit 9: CIP Program Performance Management Approach



Based on the National Strategy for Homeland Security and HSPD-7, the goals of the CIP Program are:⁷

- ❑ **Awareness** – Identify and assess the vulnerability of the nation's CI/KR
- ❑ **Protection** – Assure the protection of the nation's CI/KR from terrorist attack
- ❑ **Partnership** – Establish a collaborative environment across all levels of government and with the private sector to better protect the nation's CI/KR
- ❑ **Coordination** – Coordinate and integrate, as appropriate, with other federal emergency management and preparedness activities, including the National Response Plan.

The CIP Program will be measured against these goals. Resources will be allocated to those activities that best accomplish CIP goals, and activities that are not advancing goals will be redesigned or eliminated over time.

Metrics Definitions

Three types of metrics will be tracked for the CIP Program: **descriptive metrics**, **process metrics**, and **outcome metrics**.

- ❑ **Descriptive metrics** are necessary to understand sector resources and activity, but they do not reflect CIP performance. For instance, how many assets are there, by asset class (e.g., by transportation mode)? It may also be necessary to know the fraction of assets owned by the private sector, since this may influence how protective actions are funded.
- ❑ **Process metrics** measure whether specific activities that are important to the execution of a program were performed as planned, track the progression of a task, or

⁷ The February 2003 "National Strategy for Homeland Security" identified three objectives: (1) prevent terrorist attacks within the United States; (2) reduce America's vulnerability to terrorism; and (3) minimize the damage and recover from attacks that do occur. Paragraph 27 of HSPD-7, which sets forth the NIPP, reiterates these objectives and further emphasize the need for partnership and coordination across stakeholders and Plans.

report on the output of a process such as inventorying assets. For example, was screening equipment installed in each airport by the planned date? How many electric utilities performed vulnerability assessments this year? Process metrics are also referred to as output metrics.

- ❑ **Outcome metrics** track progress towards a strategic goal in terms of beneficial results rather than level of activity. An example of an outcome metric may be the change in number of facilities assessed as high-risk, following the implementation of protective actions.

The CIP Program will be quantified using metrics of each type. Process metrics have an important role, showing progress toward collecting the data or completing the analyses necessary to achieve CIP goals. Process metrics build a comprehensive picture of CIP status and activities. However, outcome metrics are more valuable as they indicate progress toward specific objectives and better support CIP investment decision-making. As the CIP Program matures, process metrics will be de-emphasized in favor of outcome metrics.

Some sectors are already successfully using outcome metrics to improve their CIP programs. IAIP intends to identify those best practices and adapt them to other sectors as appropriate.

A. CIP Metrics

Metrics for the CIP Program will fall into two groups—core CIP metrics and sector-specific metrics. Like the CIP Program, the metrics discussed below are expected to evolve as DHS and sector stakeholders become more knowledgeable on their specific CIP challenges.

1. Core CIP Metrics

Core CIP metrics, which will be common to all sectors, are a small set of descriptive, process, and outcome metrics that will measure initial progress in Sector-Specific Plan implementation. These metrics are aligned with the key steps in the CIP Program implementation process, as illustrated in Exhibit 10.

Exhibit 10: Core Metrics by CIP Program Implementation Process

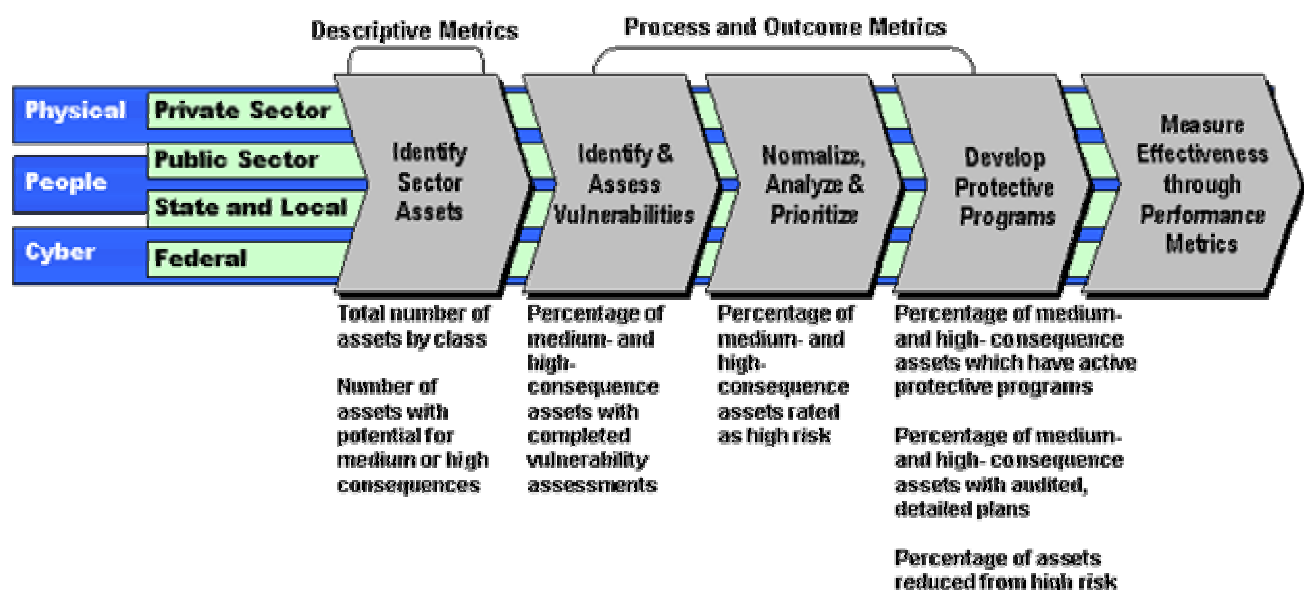


Exhibit 11 provides additional detail on these metrics.

Exhibit 11: Core Metrics

Type of Metric	Metric	Description
Descriptive	1. Total number of assets by class	This measure will be assessed for each asset class identified by the SSA. Asset classes will be different for each different critical infrastructure sector. For example, transportation asset classes represent the different modes.
Descriptive	2. Number of assets with potential for medium or high consequences	This measure will be assessed for each asset class as identified by the SSA. Tracking this metric will help determine which sectors are in the most need of assessing vulnerabilities and if there are particularly critical regions or industries. The identification of medium- and high-consequence assets is called for in the second part of the Sector-Specific Plan (Identifying Sector Assets).
Process	3. Percentage of medium- and high-consequence assets with completed vulnerability analyses	This measure will be assessed for each asset class as identified by the SSA. Tracking this measure will help determine progress against vulnerability assessment goals.
Outcome	4. Percentage of medium- and high-consequence assets rated as high risk	This measure will be assessed for each asset class as identified by the SSA. Tracking this metric will help in determining which sectors require programs to increase protection. It can help focus government and private resources on those sectors, regions and industries, with the highest identified risks first. The identification of high-risk assets is called for in the third part of the Sector-Specific Plan (Assessing Vulnerabilities and Prioritizing Assets, Exhibit 8).
Process	5. Percentage of medium- and high-consequence assets that have active protective programs to measurably reduce risk	This measure will be assessed for each asset class. Tracking this metric, 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.
Process	6. Percentage of medium- and high-consequence assets that have been assessed for readiness, response, and recovery capability	This metric should be applied to each asset class as identified by the SSA. Tracking this measure will provide insight into the degree to which readiness, response, and recovery planning is in place for the more important assets.
Outcome	7. Percentage of assets reduced from high risk	This measure should be applied to each asset class as identified by the SSA. Tracking this measure will provide insight into the effectiveness of the programs implemented to reduce risk. Programs will reduce risk through a variety of means, such as creating a better response and recovery capability for the asset, or increasing the difficulty of attacking critical infrastructure assets, or decreasing the probability of success of an attack against the asset via a variety of prevention and/or protective programs.

The SSA should describe the process for assessing these metrics. As part of this description, the following information should be included:

- ❑ How will assessment of the metric be performed (e.g., by on-site survey, statistical sample, etc.)?
- ❑ Over what period of time will the assessment of the metric be completed?

- ❑ Who/what organization will do the assessment (e.g., owners, state or local officials, the SSA, DHS, or independent organizations)?

2. Sector-Specific Goals and Metrics

In addition to the core metrics, each Sector-Specific Plan should also include development of sector-specific metrics. The SSA should define its CIP goals and provide a short, focused, and manageable list of process and outcome metrics, organized by asset class if appropriate. These goals and metrics will differ by sector, depending upon the maturity of the existing CIP program and specific characteristics of sector assets and operations. As with the core metrics, SSAs should indicate how, when, and by whom the metric will be assessed.

SSAs should strive for outcome metrics. The principal intended outcome of sector CIP programs is the reduction of risk through reducing vulnerability, potential consequences, or the likelihood of attacks. Sectors with mature risk assessment methods should define risk-based outcome measures.

DHS is committed to a metrics-based system of mission performance. For this reason, these metrics, the underpinning data, and their use in a statistically valid manner should be certified by an appropriate independent entity. This guidance is not presenting a specific auditing approach at this time. DHS will work with SSAs to develop an auditing/certification process to validate the assessment of CIP metrics.

Other intended outcomes could include:

- ❑ Reducing the cost of protective actions (e.g., lower-cost baggage screening)
- ❑ Maximizing the operating efficiency of assets with protective actions in place (e.g., lower wait times at airport checkpoints)
- ❑ Increasing public confidence in the security of sector activities (e.g., traveler confidence).

This page intentionally blank

VI. Planning for Research and Development

One of the implementation requirements of HSPD-7 is the development of an annual R&D plan on CI/KR protection. This section provides instructions for completing Part VI of the Sector-Specific Plan, which addresses R&D planning. It addresses not only hard science, but also people-oriented R&D.

Purpose: This part of the Plan explains how R&D considerations will be incorporated into the NIPP. It explains the roles of SSAs, DHS IAIP, DHS S&T, and OSTP in developing sector-specific summaries of R&D plans.

Benefits: Many CIP challenges call for science and technology solutions. The Federal CIP R&D Plan will inventory current federal R&D initiatives that have potential CIP applications, indicate technology requirements, identify gaps, and indicate planned R&D initiatives. It will also identify issues that may benefit from the initiatives of industry or academia.

Elements:

- VI. Planning for Research and Development
 - A. Sector Technology Requirements
 - B. Current R&D Initiatives
 - C. Gaps
 - D. Candidate R&D Initiatives

Organizational Responsibilities for the CIP R&D Plan

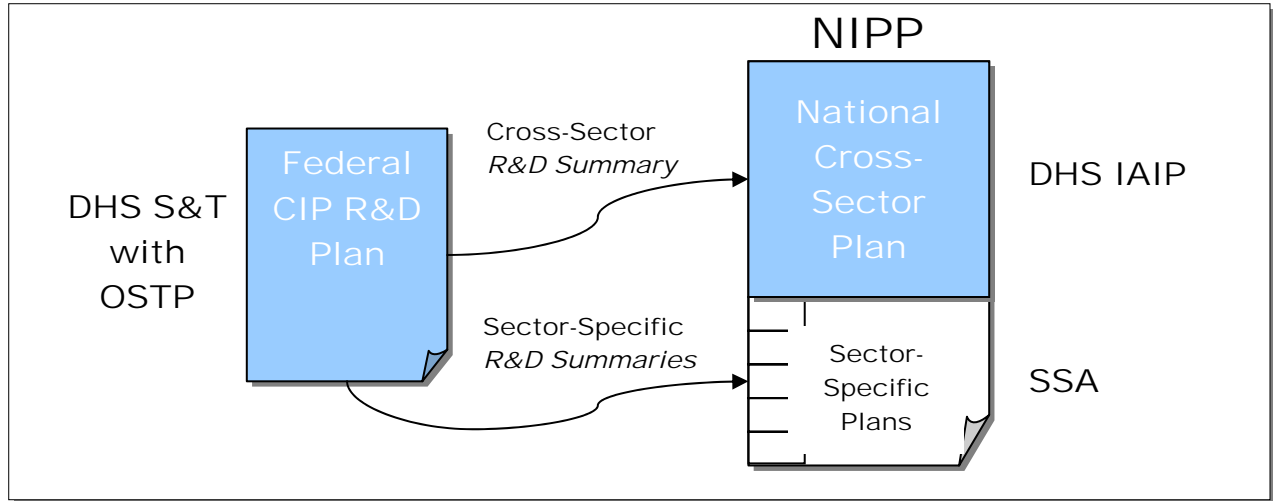
The DHS Science and Technology (S&T) Directorate is leading the development of the first annual Federal CIP R&D Plan. S&T is coordinating with the Infrastructure Subcommittee of the National Science and Technology Council of OSTP. The Subcommittee has physical and cyber security subgroups that are together forming an integrated R&D Plan. They are engaging all federal agencies to identify R&D initiatives with potential CIP applications. They will engage SSAs to identify CIP requirements that may be fulfilled by technology.

This NIPP guidance does not generate an R&D planning requirement separate from the effort being led by DHS S&T. Instead, for the NIPP, each SSA will “import” a sector-specific R&D summary based on the Federal CIP R&D Plan. The SSA will develop this summary supported by S&T and based on the Federal CIP R&D Plan. IAIP will develop the cross-sector R&D summary supported by S&T and based on the Federal CIP R&D Plan. This relationship is shown in Exhibit 12.

R&D Planning Process

S&T/OSTP have identified nine themes, such as *protection*, *detectors & sensors*, and *managing insider threats*. Each theme has physical and cyber aspects to be addressed in an integrated manner. S&T/OSTP are inventorying all federal R&D initiatives, current and planned, to identify potential CIP applications. They are working with SSAs and other sector stakeholders to identify technology requirements. They will identify gaps between requirements and current initiatives. They will indicate how planned R&D initiatives fill the gaps and will propose new R&D initiatives to fill remaining gaps.

Exhibit 12: Relationship of the Federal CIP R&D Plan to the NIPP



S&T/OSTP will map theme-based R&D requirements, initiatives, and gaps to CI/KR sectors so that SSAs can understand technology opportunities and contribute to prioritizing R&D initiatives. Note that most requirements relate to multiple sectors. For instance, sensors for biological agents would support postal operations, ports, water facilities, and emergency responders.

A. Sector Technology Requirements

In this section, SSAs should provide a description of the processes they will use to identify sector technology requirements and communicate them to S&T/OSTP for inclusion in the Federal CIP R&D Plan on an annual basis. The processes should ensure that requirements will be identified by theme. The information required from SSAs will include a summary of technology requirements in their sector chapters, highlighting requirements without the more detailed explanations included in the Federal CIP R&D Plan.

B. Current R&D Initiatives

SSAs should describe the process they will follow to annually solicit from S&T/OSTP a listing of current federal R&D initiatives that have potential to meet their sector's CIP challenges. In this section of the Plan, the SSAs should then describe how they will analyze this listing with the help of S&T and sector stakeholders and how they will indicate which initiatives have the greatest potential for positive impact. The process should ensure that impacts align with the performance measures as described in Part VI of the Sector-Specific Plans.

C. Gaps

The Plan should address how SSAs will solicit from S&T/OSTP an analysis of the gaps between the sector's technology needs and current R&D initiatives. S&T will determine these gaps as opposed to each sector doing so independently, because gaps will often be shared by multiple sectors. In this section, SSAs will describe the process by which they will summarize

the most important gaps for their sector, as identified by S&T. The roles of different parties within the sector in making this determination should be described.

D. Candidate R&D Initiatives

The Plan should also describe how SSAs will solicit from S&T/OSTP descriptions of candidate R&D initiatives to fill gaps. S&T can view cross-sector technology gaps holistically, and can identify opportunities for an initiative sponsored by one sector to support other sectors. This will focus R&D investments on the highest national CIP priorities and identify multiple-use technology solutions. In this section, SSAs will summarize the process by which they will determine which candidate R&D initiatives are most relevant for their sectors, as identified by S&T and how these will be summarized.

This page intentionally blank

5. Sector-Specific Plan Template

Enclosed with this guidance document is a CD-ROM containing a common template that SSAs can use in completing and submitting their Sector-Specific Plans to DHS. The template mirrors the organization of the plan and instructions presented in the two previous chapters of this guidance, respectively.