

REVISED DRAFT NIPP V2.0

National Infrastructure Protection Plan

Base Plan

January 2006

This document is a For-Comment-Only draft that is being provided solely to effect the extensive coordination with Federal departments and agencies; State, local, and tribal government entities; and the private sector that is required for the development of the National Infrastructure Protection Plan.

Preface

The ability to protect the critical infrastructures and key resources (CI/KR) of the United States is vital to our national security, economic vitality, and way of life. U.S. policy focuses on the importance of enhancing CI/KR protection to ensure that essential governmental missions, public services, and economic functions are maintained in the event of a terrorist attack, natural disaster, or other type of incident, and that elements of CI/KR are not exploited for use as weapons of mass destruction against our people or institutions.

The President directed me to coordinate and implement national initiatives and develop a national plan to unify and enhance CI/KR protection efforts through an unprecedented partnership involving the private sector, as well as Federal, State, local, and tribal governments. The National Infrastructure Protection Plan (NIPP) meets the requirements that the President set forth in Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection, and provides the overarching approach for integrating the Nation's many critical infrastructure protection initiatives into a single, national effort.

The NIPP provides the coordinated approach that will be used to establish national priorities, goals, and requirements for CI/KR protection so that Federal funding and resources are applied in the most effective manner to reduce vulnerability, deter threats, and minimize the consequences of attacks and other incidents. It establishes the overarching concepts relevant to all CI/KR sectors identified in HSPD-7, and addresses the physical, cyber, human, and international dimensions required for effective implementation of comprehensive programs. The Plan specifies the key initiatives, milestones, and metrics required to achieve the Nation's CI/KR protection mission. It sets forth a comprehensive risk management framework and clearly defined roles and responsibilities for the Department of Homeland Security (DHS); Sector-Specific Agencies; and other Federal, State, local, tribal, and private sector security partners.

The NIPP was developed through extensive coordination with security partners at all levels of government and the private sector. Continued cooperation and collaboration between and among these security partners is critical to the successful implementation of this Plan. The Letter of Instruction included in the NIPP provides specific implementation guidance for all security partners. I ask for your continued commitment and cooperation as we move forward to identify the resources and the processes needed to implement the NIPP and to protect the Nation's CI/KR.

Michael Chertoff
Secretary
Department of Homeland Security

Letter of Agreement

The National Infrastructure Protection Plan (NIPP) provides the unifying structure for the integration of critical infrastructures and key resources (CI/KR) protection efforts into a single national program. The NIPP provides an overall framework integrating programs and activities that are currently underway in the various sectors, as well as new and developing CI/KR protection efforts. This collaborative effort between the private sector; State, local, and tribal governments; non-governmental organizations; and the Federal government will result in the prioritization of protection initiatives and investments across sectors to ensure that resources are applied where they offer the most benefit for reducing risk by lowering vulnerabilities, deterring threats, and minimizing the consequences of attacks and other incidents.

By signing this letter of agreement, Homeland Security Presidential Directive 7 (HSPD-7) designated Sector-Specific Agencies and other Federal departments and agencies with special functions related to CI/KR protection commit to:

- Support NIPP concepts, framework, and processes, and carry out their assigned functional responsibilities regarding the protection of CI/KR as described herein.
- Work with the Secretary of Homeland Security, as appropriate and consistent with their own agency-specific authorities, resources, and programs, to coordinate funding and implementation of programs that enhance CI/KR protection;
- Cooperate and coordinate with the Secretary of Homeland Security, in accordance with guidance provided in HSPD-7, as appropriate and consistent with their own agency-specific authorities, resources, and programs, to facilitate CI/KR protection;
- Develop or modify existing interagency and agency-specific CI/KR plans, as appropriate, to facilitate compliance with the NIPP.
- Develop and maintain partnerships for CI/KR protection with appropriate State, regional, local, tribal, and international entities; the private sector; and non-governmental organizations; and
- Protect critical infrastructure information according to the Protected Critical Infrastructure Information (PCII) Program or other appropriate guidelines, and share NIPP-related information, as appropriate and consistent with their own agency-specific authorities and the process described herein.

Signatory departments and agencies follow.

1 **Signatories**

2 [Insert signatories here]

1 **Letter of Instruction**

2 This letter will contain implementation instructions.

1	Table of Contents	
2	Preface	i
3	Letter of Agreement	iii
4	Signatories.....	v
5	Letter of Instruction	vii
6	Executive Summary.....	1
7	1. Introduction	1
8	2. Authorities, Roles, and Responsibilities	1
9	3. The CI/KR Protection Program Strategy: Reducing Risk	2
10	4. Organizing and Partnering for CI/KR Protection.....	3
11	5. CI/KR Protection: An Integral Part of the Homeland Security Mission.....	4
12	6. Ensuring an Effective, Efficient Program Over the Long Term	5
13	7. Providing Resources for the CI/KR Protection Program.....	5
14	Glossary of Key Terms	7
15	1. Introduction	11
16	1.1 Purpose of the NIPP and the SSPs.....	11
17	1.2 Scope and Applicability of the NIPP	12
18	1.2.1 Scope	12
19	1.2.2 Applicability	12
20	1.3 Threats to the Nation's CI/KR.....	13
21	1.3.1 The Vulnerability of the U.S. Infrastructure to the 21 st Century	
22	Threat Environment.....	13
23	1.3.2 The Nature of Possible Terrorist Attacks.....	13
24	1.3.3 Characteristics of Terrorism	14
25	1.4 All-Hazards and CI/KR Protection	14
26	1.5 The Secretary of Homeland Security's Role in CI/KR Protection	15
27	1.6 Goal and Objectives of the NIPP.....	15
28	1.6.1 Building Security Partnerships.....	16
29	1.6.2 Implementing a Long-Term CI/KR Risk-Reduction Program	16
30	1.6.3 Maximizing Efficient Use of Resources for CI/KR Protection.....	17
31	1.7 Planning Assumptions.....	17
32	1.8 Special Considerations.....	18
33	2. Authorities, Roles, and Responsibilities	21
34	2.1 Authorities	21
35	2.2 Roles and Responsibilities	22
36	2.2.1 Department of Homeland Security	22
37	2.2.2 Sector-Specific Agencies	24

1	2.2.3	Other Federal Departments, Agencies, and Offices	26
2	2.2.4	State, Territorial, Local, and Tribal Governments	27
3	2.2.4.1	State and Territorial Governments	27
4	2.2.4.2	Local Governments	29
5	2.2.4.3	Tribal Governments	30
6	2.2.4.4	Regional Partners	30
7	2.2.5	Private Sector and Other Owners and Operators	31
8	2.2.6	Advisory Councils	32
9	2.2.7	Academia, Research Centers, and Think Tanks	33
10	3.	The Protection Program Strategy: Reducing Risk	35
11	3.1	Set Security Goals	36
12	3.2	Identify Assets	37
13	3.2.1	National Infrastructure Inventory	38
14	3.2.2	Protecting and Accessing Asset Information	39
15	3.2.3	SSA Roles in Asset Identification	40
16	3.2.4	Identifying Cyber Assets	40
17	3.3	Assess Risks	41
18	3.3.1	NIPP Baseline Criteria for Assessment Methodologies	42
19	3.3.1.1	Ensuring That Previous Assessments Can Be Used	42
20	3.3.1.2	Baseline Criteria	42
21	3.3.2	Consequence Analysis	43
22	3.3.2.1	Consequence Assessment Methodologies That Enable National	
23		Risk Analysis	43
24	3.3.2.2	Consequence Screening	44
25	3.3.3	Vulnerability Assessment	45
26	3.3.3.1	Vulnerability Assessment Methodologies That Enable National	
27		Risk Analysis	45
28	3.3.3.2	SSA and DHS Analysis Responsibilities	46
29	3.3.4	Threat Analysis	47
30	3.4	Prioritize	50
31	3.5	Implement Protective Programs	51
32	3.5.1	Protective Actions	51
33	3.5.2	Characteristics of Effective Protective Programs	52
34	3.5.3	Protective Programs, Initiatives, and Reports	54
35	3.6	Measure Effectiveness	55
36	3.6.1	NIPP Metrics and Measures	55
37	3.6.1.1	Core Metrics	56
38	3.6.1.2	Sector-Specific Metrics	56
39	3.6.2	Gathering Performance Information	56
40	3.6.3	Assessing Performance and Reporting on Progress	57
41	3.7	Using Metrics and Performance Measurement for Continuous Improvement	58

1	4.	Organizing and Partnering for CI/KR Protection	59
2	4.1	Leadership and Coordination Mechanisms	59
3	4.1.1	National-Level Coordination	59
4	4.1.2	Sector Partnership Coordination	60
5	4.1.2.1	Sector Coordinating Councils	61
6	4.1.2.2	Government Coordinating Councils	62
7	4.1.3	State, Local, and Tribal Government Coordination.....	62
8	4.1.4	Regional Coordination.....	62
9	4.1.5	International CI/KR Protection Cooperation.....	63
10	4.1.5.1	Cooperation with International Security Partners	63
11	4.1.5.2	Implementing Current Agreements	64
12	4.1.5.3	Approach to International Cybersecurity	65
13	4.1.5.4	Foreign Investment in CI/KR	65
14	4.2	Information-Sharing: A Networked Approach	66
15	4.2.1	The Homeland Security Information Network	66
16	4.2.2	The Federal Intelligence Node	69
17	4.2.3	The Federal Infrastructure Node	69
18	4.2.4	State, Local, Tribal, and Regional Node	69
19	4.2.5	Private Sector Node	70
20	4.2.6	DHS Operations Node.....	70
21	4.2.6.1	Homeland Security Operations Center	71
22	4.2.6.2	National Infrastructure Coordinating Center	72
23	4.2.6.3	National Coordinating Center for Telecommunications	72
24	4.2.6.4	U.S. Computer Emergency Readiness Team	73
25	4.2.7	Use of Other CI/KR Information-Sharing Components and Technologies.....	73
26	4.3	Protection of Sensitive CI/KR Information	74
27	4.3.1	Protected Critical Infrastructure Information Program	75
28	4.3.1.1	PCII Program Office	75
29	4.3.1.2	Critical Infrastructure Information Protection	75
30	4.3.1.3	Uses of PCII	76
31	4.3.1.4	PCII Protections and Authorized Users	76
32	4.3.2	Other Security Regimes	76
33	4.3.2.1	Sensitive Security Information (SSI).....	77
34	4.3.2.2	Unclassified Controlled Nuclear Information (UCNI)	77
35	4.3.2.3	Freedom of Information Act Exemptions and Exclusions	77
36	4.3.2.4	Classified Information.....	77
37	4.3.2.5	Physical and Cybersecurity Measures	78
38	4.4	Privacy and Constitutional Freedoms	78
39	5.	Integrating CI/KR Protection as Part of the Homeland Security Mission	81
40	5.1	A Coordinated National Approach to the Homeland Security Mission.....	81
41	5.1.1	Legislation	81
42	5.1.2	Strategies	81
43	5.1.2.1	The National Strategy for Homeland Security	81
44	5.1.2.2	The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets	82
45			

1	5.1.2.3	The National Strategy to Secure Cyberspace	82
2	5.1.2.4	The National Intelligence Strategy of the United States of America	83
3	5.1.3	Homeland Security Presidential Directives and National Initiatives	83
4	5.1.3.1	HSPD-3, Homeland Security Advisory System	83
5	5.1.3.2	HSPD-5, Management of Domestic Incidents	84
6	5.1.3.3	HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection	84
7	5.1.3.4	HSPD-8, National Preparedness.....	84
8	5.2	The CI/KR Protection Component of the Homeland Security Mission.....	85
9	5.3	Relationship of NIPP to Other CI/KR Plans and Programs	86
10	5.3.1	Sector-Specific Plans	86
11	5.3.2	State, Regional, Local, and Tribal CI/KR Protection Programs	87
12	5.3.3	Other Security Partner Plans or Programs Related to CI/KR Protection	88
13	5.4	CI/KR Protection and Incident Management	88
14	5.4.1	The National Response Plan.....	88
15	5.4.2	Transitioning From NIPP Steady-State to Incident Management	89
16	6.	Ensuring an Effective, Efficient Program Over the Long Term.....	91
17	6.1	Building National Awareness.....	91
18	6.2	Enabling Education, Training, and Exercise Programs	92
19	6.2.1	Types of Expertise for CI/KR Protection	92
20	6.2.2	Individual Education and Training	92
21	6.2.2.1	Technical CI/KR Protection Training	93
22	6.2.2.2	Academic and Research Programs.....	94
23	6.2.2.3	Continuing Education and Professional Competency	94
24	6.2.3	Organizational Training and Exercises.....	95
25	6.2.4	Security Partner Role and Approach	95
26	6.3	Conducting Research and Development.....	96
27	6.3.1	National Critical Infrastructure Protection R&D Plan	96
28	6.3.1.1	CI/KR Protection R&D Strategic Goals.....	97
29	6.3.1.2	CI/KR Protection R&D Areas.....	97
30	6.3.1.3	CI/KR Protection R&D Roadmap	98
31	6.3.1.4	Coordination of NCIP R&D Plan With SSP R&D Planning	98
32	6.3.2	Cybersecurity R&D Planning	98
33	6.3.3	Other R&D That Supports CI/KR Protection.....	99
34	6.3.4	Technology Pilot Programs	99
35	6.4	Building and Maintaining Databases, Simulations, and Other Tools	100
36	6.4.1	National CI/KR Protection Data Systems	100
37	6.4.2	Simulation and Modeling	101
38	6.4.3	Coordination With Security Partners on Databases and Modeling	102
39	6.5	Continuously Improving the NIPP and the SSPs.....	103
40	6.5.1	Management and Coordination	103
41	6.5.2	Maintenance and Updating	103

1	7.	Providing Resources for the CI/KR Protection Program.....	105
2	7.1	The Risk-Based Resource Allocation Process	105
3	7.1.1	Sector-Specific Agency Reporting to DHS	106
4	7.1.2	State Government Reporting to DHS	106
5	7.1.3	Aggregating Submissions to DHS	107
6	7.2	Federal Resource Allocation Process for DHS, SSAs, and Other Federal Agencies	107
7	7.2.1	Department of Homeland Security	108
8	7.2.2	Sector-Specific Agencies	108
9	7.2.3	Executive Office of the President	109
10	7.2.4	Summary of Roles and Responsibilities	109
11	7.3	Federal Resources for State and Local Government Preparedness	110
12	7.4	Setting an Agenda in Collaboration With CI/KR Protection Security Partners	112
13		List of Acronyms and Abbreviations.....	113
14		Appendices	
15		Appendix 1A: Cross-Sector Cybersecurity.....	119
16		Appendix 1B: International CI/KR Protection	139
17		Appendix 2A: Summary of Relevant Statutes, Strategies, and Directives	155
18		Appendix 2B: NIPP Implementation Initiatives and Actions	163
19		Appendix 3A: NIPP Baseline Criteria for Assessment Methodologies	171
20		Appendix 3B: Existing Protective Programs and Other In-Place Measures	175
21		Appendix 3C: National Asset Database.....	179
22		Appendix 4A: Existing Coordination Mechanisms.....	185
23		Appendix 4B: Protected Critical Infrastructure Information (PCII) Program	187
24		Appendix 5A: Sector Overview	193
25		Appendix 5B: Sector-Specific Plan Content Summary	201
26		Appendix 5C: State, Territorial, Tribal and Local Government Considerations.....	205
27		Appendix 5D: Recommended Homeland Security Practices for Use by the Private Sector.....	211
28		Appendix 6A: Research and Development to Improve CI/KR Protection Capabilities	213

1 **List of Figures and Tables**

2 **Figures**

3 Figure 3-1: NIPP Risk Management Framework 35

4 Figure 4-1: Sector Partnership Model 61

5 Figure 4-2: NIPP Information-Sharing Approach 67

6 Figure 5-1: National Framework for Homeland Security 82

7 Figure 5-2: Sector-Specific Plan Structure..... 86

8 Figure 7-1: DHS, SSA, and EOP Roles and Responsibilities in Federal Resource Allocation..... 109

9 **Tables**

10 Table 2-1: Sector-Specific Agencies and HSPD-7 Assigned CI/KR Sectors 24

11 Table 4-1: Currently Available HSIN COI..... 68

12 Table 1A-1: Sample Cyber Measures and Metrics 131

13 Table 3C-1: Database Integration..... 180

14

Executive Summary

1. Introduction

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

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

Enhance protection of the Nation's CI/KR in order to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and enable national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.

The NIPP provides the unifying structure for the integration of existing and future CI/KR protection efforts into a single national program to achieve this goal. Protection includes actions to guard or shield CI/KR assets, systems, networks, or their interconnecting links from exposure, injury, destruction, incapacitation, or exploitation. In the context of the NIPP, this includes actions to deter, mitigate, or neutralize the threat, vulnerability, or consequences associated with a terrorist attack or other incident.

This program focuses on three principal objectives:

- Building security partnerships to implement CI/KR protection programs;
- Implementing a long-term risk-reduction program; and
- Maximizing efficient use of resources for CI/KR protection.

These objectives require a collaborative partnership between and among a diverse set of security partners, including the Federal government, private sector; State, local, and tribal governments; international entities; and non-governmental organizations. The NIPP provides the framework that defines the processes and mechanisms that these security partners will use to develop and implement the national program to protect CI/KR across all sectors over the long term. The NIPP framework will enable the prioritization of protection initiatives and investments across sectors to ensure that resources are applied where they offer the most benefit for reducing risk by lessening vulnerabilities, deterring threats, and minimizing the consequences of terrorist attacks and other man-made and natural disasters.

2. Authorities, Roles, and Responsibilities

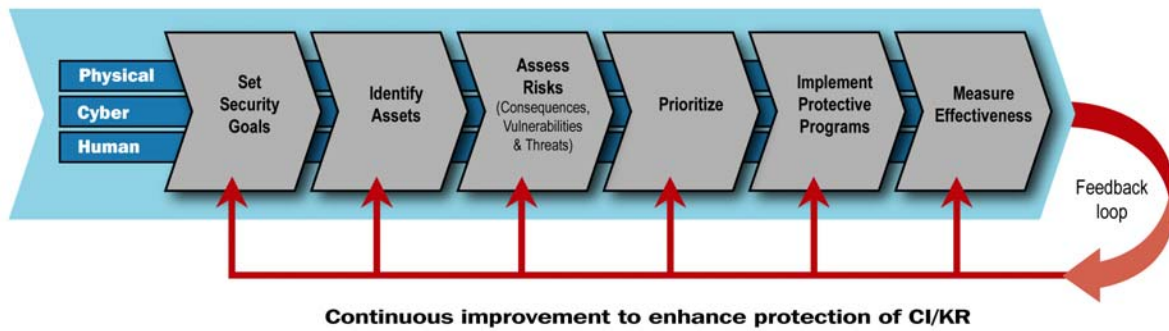
The Homeland Security Act of 2002 provides the primary authority for the overall homeland security mission and provides the basis for Department of Homeland Security (DHS) responsibilities in the

1 protection of the Nation's CI/KR. The Act assigns DHS the responsibility to develop a comprehensive
2 national plan for securing CI/KR and for recommending "measures necessary to protect the key resources
3 and critical infrastructure of the United States in coordination with other agencies of the Federal
4 government and in cooperation with State and local government agencies and authorities, the private
5 sector, and other entities." The NIPP delineates roles and responsibilities for security partners in carrying
6 out these activities while respecting the authorities, jurisdictions, and prerogatives of these partners.
7 Primary roles include:

- 8 • **Department of Homeland Security:** Manage the Nation's overall CI/KR protection framework and
9 oversees NIPP implementation.
- 10 • **Sector-Specific Agencies:** Implement the NIPP framework and guidance in designated CI/KR sectors.
- 11 • **Other Federal Departments, Agencies, and Offices:** Implement specific CI/KR protection roles
12 designated in HSPD-7 or other relevant statutes and executive orders and policy directives.
- 13 • **State, Territorial, Local, and Tribal Governments:** Develop and implement a CI/KR protection
14 program as a component of their overarching homeland security programs.
- 15 • **Regional Partners:** Use partnerships that cross jurisdictional and sector boundaries to address CI/KR
16 protection within a defined geographical area.
- 17 • **Private Sector Owners and Operators:** Undertake CI/KR protection, coordination, and cooperation
18 activities, as necessary.
- 19 • **Homeland Security Advisory Councils:** Provide advice, recommendations, and expertise to the
20 government regarding protection policy and activities.
- 21 • **Academia, Research Centers, and Think Tanks:** Provide CI/KR protection subject matter expertise,
22 independent analysis, research and development, and educational programs.

23 3. The CI/KR Protection Program Strategy: Reducing Risk

24 The cornerstone of the NIPP is its risk management framework that establishes the processes for
25 combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and
26 rational assessment of national or sector risk. The results of these processes drive CI/KR risk-reduction
27 activities. The framework applies to the general threat environment, as well as to specific threats or incident
28 situations. DHS and the Sector-Specific Agencies share responsibilities for implementing the risk
29 management framework.



Continuous improvement to enhance protection of CI/KR

NIPP Risk Management Framework

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

4. Organizing and Partnering for CI/KR Protection

The NIPP defines the organizational structures that provide coordination for CI/KR protection at all levels of government, as well as within and across sectors. Sector-specific planning and coordination are addressed through a Private Sector Coordinating Council and a Government Coordinating Council for each sector. These councils create a structure through which representative groups from all levels of government and the private sector can collaborate and develop consensus approaches to CI/KR protection. DHS also works with security partners as they establish cross-sector bodies for coordination, communication, and best practice sharing across CI/KR sectors within each jurisdiction or geographic areas. Cross-sector issues and interdependencies will be addressed between the SCCs through the Partnership for Critical Infrastructure Security. The Partnership for Critical Infrastructure Security membership is comprised of one or more members and their alternates from each of the Sector Coordinating Councils. The corollary NIPP Federal Senior Leadership Council is comprised of one or more representatives and their alternates from each individual Government Coordinating Council. These cross-sector bodies will convene in joint session, as appropriate, to address cross-cutting CI/KR protection issues.

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

1 NIPP implementation relies on critical infrastructure information provided by the private sector. Much of this
2 is sensitive business or security information that could cause serious damage to the economy, public
3 safety, or security if unauthorized disclosure or access to this information takes place. The Federal
4 government has a statutory responsibility to safeguard information collected on infrastructure security-
5 related activities. DHS and other Federal agencies use a number of programs and procedures, such as the
6 Protected Critical Infrastructure Information (PCII) Program, to ensure that security-related information is
7 properly safeguarded. These programs and procedures relate to sensitive security information for
8 transportation activities, unclassified controlled nuclear information, contractual provisions, classified
9 national security information, law enforcement information, and other requirements established by law.

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

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

14 The Homeland Security Act; the National Strategies for Homeland Security, Physical Protection of Critical
15 Infrastructures and Key Assets, and for Securing Cyberspace; and a series of Homeland Security
16 Presidential Directives, most importantly Homeland Security Presidential Directive 7 (HSPD-7), provide the
17 authority for the measures outlined in the NIPP. These documents work together to provide a coordinated
18 national approach to homeland security that is based on a common framework for CI/KR protection,
19 preparedness, and incident management.

20 The NIPP defines the CI/KR component of the homeland security mission. Implementing this component
21 requires partnerships, coordination, and collaboration between all levels of government and the private
22 sector. To enable this, the NIPP provides guidance on the structure and content of each sector's CI/KR
23 plan, as well as the CI/KR protection-related aspects of State and local homeland security plans. This
24 provides a national-level framework for each individual sector that informs the development,
25 implementation, and updating of State and local homeland security strategies and CI/KR protection
26 programs.

27 To be effective, the NIPP must complement other plans designed to help prevent, prepare for, protect
28 against, respond to, and recover from terrorist attacks, natural disasters, and other emergencies. The NIPP
29 and the National Response Plan (NRP) work together to provide a comprehensive, integrated approach to
30 the homeland security mission. The NIPP establishes the overall risk-based approach that defines the
31 Nation's CI/KR steady-state protective posture, while the NRP provides the approach for domestic incident
32 management. Step-ups in CI/KR protective measures that correspond to the threat levels established in the
33 Homeland Security Advisory System (HSAS) provide the bridge between NIPP steady-state protection and
34 incident management activities using the NRP. This link between the evolving threat environment and
35 corresponding levels of protection provides the means to transition from the steady-state processes
36 detailed in the NIPP to the incident management processes described in the NRP.

37 When an Incident of National Significance occurs, the NRP is implemented to guide overall coordination of
38 domestic incident management activities. NIPP partnerships and processes provide the CI/KR dimension of
39 this Plan, complementing NRP incident management and facilitating those actions directly related to the
40 current threat status, incident prevention, response, restoration, and recovery.

6. Ensuring an Effective, Efficient Program Over the Long Term

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

- **National awareness** to support the sustainability of the CI/KR protection program, security investments, and protection activities by ensuring a broad understanding by the public, business, and government of the multi-hazard threat environment and of what is being done to protect the Nation's CI/KR against such threats.
- **Education and training** to ensure that skilled and knowledgeable professionals are available to undertake NIPP-related responsibilities in the future.
- **Research and development** to improve protective capabilities or to dramatically lower the costs of existing capabilities so that sector security partners can afford to do more with limited budgets.
- **Building and maintaining** the currency of databases and data systems to enable continuously refined risk assessment within and across sectors and to ensure preparedness for domestic incident management.
- **Continuously improving** the NIPP and associated plans and programs through ongoing management and maintenance activities.

7. Providing Resources for the CI/KR Protection Program

Prioritizing the allocation of Federal resources through the annual budget process involves multiple Federal agencies, the Homeland Security Council (HSC), and the Office of Management and Budget (OMB). The Federal resource allocation process for CI/KR protection funding starts with establishing sector requirements, which are then prioritized based on their criticality to the Nation. Protective programs that have the greatest potential for reducing risk are then recommended. The HSC reviews proposed funding, resolves outstanding policy issues, and works with the various Federal agencies to finalize recommendations to be passed to OMB by the various Federal departments and agencies for inclusion in the President's budget submission. The annual budget process informs decisions affecting Federal government protective programs and Federal grants to State, Territorial, local, and tribal government entities; it can also help inform State, local, and private sector CI/KR planning and protection investments.

Glossary of Key Terms

All-Hazards. An approach for prevention, protection, preparedness, response, and recovery that addresses the full range of threats, including domestic terrorist attacks, natural and man-made disasters, and emergencies.

Asset. As defined in the Homeland Security Act of 2002, assets include contracts, facilities, property, records, unobligated or unexpended balances of appropriations, and other funds or resources (other than personnel).

Consequence. The result of a terrorist attack or other incident that reflects the level, duration, and nature of the loss resulting from the incident. For the purposes of the NIPP, these consequences are divided into four main categories:

- **Health Impact:** Effect on human life and physical well-being (e.g., fatalities, injuries).
- **Economic Impact:** Direct and indirect effects on the economy (e.g., cost to rebuild asset, cost to respond to and recover from attack, downstream costs resulting from unavailability of product or service).
- **Psychological Impact:** Effect on the public's morale and confidence in national economic and political institutions.
- **Governance Impact:** Effect on the government's ability to maintain order, deliver minimum essential public services, ensure the public's health and safety, and carry out national security-related missions.

Control Systems: Computer-based systems used within many infrastructures and industries to monitor and control sensitive processes and physical functions. These systems typically collect measurement and operational data from the field, process and display the information, and relay control commands to local or remote equipment or human-machine interfaces (operators). Examples of types of control systems include Supervisory Control and Data Acquisition (SCADA) systems, Process Control Systems (PCS), and Digital Control Systems (DCS).

Critical Infrastructure. Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such assets, systems, networks, or functions would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Critical Infrastructure Information (CII). As defined by the Critical Infrastructure Information Act of 2002, CII includes information not customarily in the public domain and related to the security of critical infrastructure or protected systems.

Cybersecurity. The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure the information's confidentiality, integrity, and availability.

Dependency. The one-directional reliance of an asset, sector, or sectors on other input, interaction, or other requirement in order to function properly.

Government Coordinating Council (GCC). The government counterpart to the Sector Coordinating Council for each sector that is established to enable interagency coordination. The GCC is comprised of representatives across various levels of government (Federal, State, Territorial, local, and tribal) as appropriate to the security landscape of each individual sector.

Hazard. Something that is potentially dangerous or harmful, often the root cause of an unwanted outcome.

Infrastructure. As defined in Executive Order 13010, infrastructure is the framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole. Consistent with the definition of assets in the Homeland Security Act, infrastructure assets include of one or more of the following elements:

- **Physical elements:** Tangible property such as facilities, components, real estate, animals, and products.
- **Cyber elements:** Electronic information and communications systems and the information contained in those systems. Information and communications systems are comprised of all the hardware and software that processes (i.e., creates, accesses, modifies, and destroys), stores (e.g., all media types: paper, magnetic, and electronic), and communicates (i.e., shares and distributes) information, or any combination of all of these elements.
- **Human elements:** Critical knowledge, expertise, or functions of people (i.e., tacit knowledge and job expertise or skills) uniquely susceptible to destruction, incapacitation, or exploitation through the individuals who possess or use such knowledge.

Interdependency. The reliance of an asset, sector, or sectors on other assets or sectors to function properly, and their reliance on the original entity in return. This reliance is reciprocal and, at a minimum, bidirectional.

Key Assets. Individual targets whose destruction could cause large-scale injury, death, or destruction of property, and/or profoundly damage national prestige, and confidence.

Key Resources. As defined in the Homeland Security Act of 2002, key resources are publicly or privately controlled resources essential to the minimal operations of the economy and government.

Network. In the context of the NIPP, a network is a group of assets or systems that share information or interact with each other in order to provide infrastructure services to the Nation.

Normalize. In the context of the NIPP, to normalize is the process of transforming risk data into comparable units.

Preparedness. The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from domestic incidents. Preparedness is a continuous process involving efforts at all levels of government and between government and private sector and non-governmental organizations to identify threats, determine vulnerabilities, and identify required resources.

Prevention. Actions taken to avoid an incident or to intervene to stop an incident from occurring. Prevention involves actions taken to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; immunizations, isolation, or quarantine; public health and agricultural surveillance and testing processes; and, as appropriate, specific law enforcement operations aimed at deterring, preempting, interdicting, or disrupting illegal activity and apprehending potential perpetrators and bringing them to justice.

Prioritize. In the context of the NIPP, to prioritize is the process of using risk assessment results to identify where risk-reduction efforts are most needed and subsequently determine which protective actions should be instituted in order to have the greatest effect.

Protection. Actions to guard or shield CI/KR assets, systems, networks, or their interconnecting links from exposure, injury, destruction, incapacitation, or exploitation. In the context of the NIPP, protection includes actions to deter, mitigate, or neutralize the threat, vulnerability, or consequences associated with a terrorist attack or other incident. Protection can include a wide range of activities, including hardening facilities, building resiliency and redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing security systems, and implementing strict security measures.

Recovery. The development, coordination, and execution of service- and site-restoration plans for impacted communities and the reconstitution of government operations and services through individual, private sector, non-governmental, and public assistance programs that identify needs and define resources; provide housing and promote restoration; address long-term care and treatment of affected persons; implement additional measures for community restoration; incorporate mitigation measures and techniques, as feasible; evaluate the incident to identify lessons learned; and develop initiatives to mitigate the effects of future incidents.

Response. Activities that address the short-term, direct effects of an incident. Includes immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution of emergency operations plans and incident mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into the nature and source of the threat; ongoing surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at preempting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.

Risk. A measure of potential harm that encompasses threat, vulnerability, and consequence. In the context of the NIPP, risk is the potential for loss, damage, or disruption to the Nation's CI/KR resulting from destruction, incapacitation, or exploitation during some future man-made or naturally occurring event.

Risk Management Framework. A planning methodology that outlines the process for setting security goals, identifying assets, assessing risks, prioritizing and implementing protective programs, and measuring effectiveness to produce a comprehensive, systematic, and rational assessment of national or sector risk that drives CI/KR risk-reduction activities.

Sector. A logical collection of assets that provides a common function to the economy, government, or society. The NIPP addresses 17 CI/KR sectors as defined by HSPD-7.

Sector Coordinating Council (SCC). Self-organized, self-run, and self-governed organizations that are fully representative of a spectrum of key stakeholders within a sector that serve as the government's principal point of entry into each sector for developing and coordinating a wide range of infrastructure protection activities and issues.

Sector Partnership Model. The framework for key security partners in the private sector, Federal agencies, States, Territories, local governments, and tribes to work together seamlessly in robust public-private partnerships.

Sector-Specific Agency (SSA). Federal departments and agencies identified under HSPD-7 as responsible for the protection activities in specified CI/KR sectors.

Sector-Specific Plan (SSP). Augmenting plans that complement and extend the NIPP Base Plan and detail the application of the NIPP core processes specific to each CI/KR sector. SSPs are developed by the SSAs in coordination with other security partners.

Security Partner. A Federal, State, regional, Territorial, local, or tribal government entity, private sector owners and operators of infrastructure, academic and professional entities, and certain not-for-profit and private volunteer organizations that share in the responsibility for protecting the Nation's CI/KR.

Steady-State. In the context of the NIPP, steady-state is the posture for routine, normal, day-to-day operations as contrasted with temporary periods of heightened alert or real-time response to threats or incidents.

System. In the context of the NIPP, a system is a collection of assets, resources, or elements that performs a process that provides infrastructure services to the Nation.

Terrorism. As defined in the Homeland Security Act of 2002, terrorism includes any activity that: (1) involves an act that is (a) is dangerous to human life or potentially destructive of critical infrastructure or key resources, and (b) a violation of the criminal laws of the United States or of any State or other subdivision of the United States; and (2) appears to be intended to (a) intimidate or coerce a civilian population, (b) influence the policy of a government by intimidation or coercion, or (c) affect the conduct of a government by mass destruction, assassination, or kidnapping.

Threat. An indication of possible violence, harm, or danger that includes both intent and capabilities. In the context of the NIPP, a threat is the likelihood that a particular target, or type of target, will suffer an attack or incident; for terrorist attack, threat likelihood is based on the analysis of the intent and capability of an adversary.

Vulnerability. A weakness in the design, implementation, or operation of an asset or system that can be exploited by an adversary or disrupted by a natural hazard.

1. Introduction

Protecting the critical infrastructures and key resources (CI/KR) of the United States is essential to the Nation's security, economic vitality, and way of life. CI/KR includes the assets, systems, networks, and functions that provide vital services to the Nation. Terrorist attacks on CI/KR and other man-made and natural disasters could significantly disrupt the functioning of government and business alike, and produce cascading effects far beyond the affected CI/KR sector and physical location of the incident. Direct attacks could result in large-scale human casualties, property destruction, and economic damage and also profoundly damage national prestige, morale, and confidence. Terrorist attacks using components of the Nation's CI/KR as weapons of mass destruction¹ could have even more devastating physical, psychological, and economic consequences.

The protection of the Nation's CI/KR, therefore, is an essential part of the homeland security mission of making America safer, more secure, and more resilient from terrorist attacks and other natural and man-made hazards. Protection includes actions to guard or shield CI/KR assets, systems, networks, or their interconnecting links from exposure, injury, destruction, incapacitation, or exploitation. In the context of the NIPP, this includes actions to deter, mitigate, or neutralize the threat, vulnerability, or consequences associated with a terrorist attack or other incident. Protection can include a wide range of activities including hardening facilities, building resiliency and redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing security systems, and implementing strict security measures. The National Infrastructure Protection Plan (NIPP) and its complementary Sector-Specific Plans (SSPs) provide a consistent, unifying structure for integrating both existing and future CI/KR protection efforts. It also provides the core processes and mechanisms to enable government and private sector security partners to work together to implement CI/KR protection initiatives.

1.1 Purpose of the NIPP and the SSPs

The NIPP provides the framework for the unprecedented cooperation that is needed to develop, implement, and maintain a coordinated national effort that brings together government at all levels, the private sector, and international organizations and allies. In addition, the SSPs mandated by the NIPP detail the application of the NIPP framework to each CI/KR sector. SSPs are developed by the designated Federal Sector-Specific Agencies (SSAs) in coordination with sector security partners.

Together, these plans provide the mechanisms for identifying assets, systems, and networks; understanding threats, assessing vulnerabilities and consequences; prioritizing protection initiatives and investments based on costs and benefits so that they are used where they offer the greatest reduction of risk; and implementing information-sharing and protection measures within and across CI/KR sectors.

The NIPP also delineates the roles and responsibilities for carrying out these activities while respecting the authorities, jurisdictions, and prerogatives of the various public and private sector security partners

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

involved. Implementing the NIPP will involve the integrated and coordinated support of all security partners with infrastructure protection responsibilities across the country and internationally.

1.2 Scope and Applicability of the NIPP

This section describes the overall scope and applicability of the NIPP. While the NIPP covers the full range of physical and cyber protection within and across all of the Nation's CI/KR sectors, it is applicable to the various public and private sector security partners in different ways.

1.2.1 Scope

In accordance with the policy direction established in Homeland Security Presidential Directive 7 (HSPD-7), the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, and the National Strategy to Secure Cyberspace, the NIPP focuses specifically on the protection of CI/KR from the unique and potentially catastrophic impacts of terrorist attacks. At the same time, the NIPP builds on and is structured to be consistent with and supportive of the Nation's all-hazards approach to homeland security preparedness and domestic incident management.

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

1.2.2 Applicability

The NIPP covers the full range of CI/KR sectors as defined in HSPD-7. The framework is applicable to all security partners with CI/KR protection responsibilities and includes explicit roles and responsibilities for the Federal government, including CI/KR under the control of the legislative, executive, or judicial branches. Federal departments and agencies with specific responsibilities for CI/KR protection are required to take actions in accordance with the NIPP. The NIPP also provides an organizational structure, protection guidelines, and recommended activities for other security partners to help ensure consistent implementation of the national framework and the most effective use of resources. State², local³, and tribal government security partners are required to establish CI/KR protection programs consistent with the National Preparedness Goal and as a condition of eligibility for certain Federal grant programs. Private sector owners and operators are encouraged to participate in the NIPP partnership model and to initiate

² Any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States. (Homeland Security Act of 2002)

³ A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government; an Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and a rural community, unincorporated town or village, or other public entity. (Homeland Security Act of 2002)

protective measures to augment existing plans for risk management, business continuity, and incident management and response in line with the NIPP framework.

1.3 Threats to the Nation's CI/KR

Presidential guidance and national strategies focus CI/KR protection efforts on addressing the emerging terrorist threat environment as an essential component of the all-hazards nature of the homeland security mission. The emergence of the terrorist threat as a reality in the 21st century presents new challenges and requires new approaches focused on intelligence-driven analyses, information sharing, and unprecedented partnerships between the public and private sector. As a result of decades of experience responding to non-catastrophic natural disasters, industrial accidents, and the deliberate acts of malicious individuals, the Nation's CI/KR are generally resilient. However, government and business contingency, incident, and emergency response plans and preparedness efforts must now also address the unique aspects of the terrorist threat and catastrophic natural disasters.

1.3.1 The Vulnerability of the U.S. Infrastructure to the 21st Century Threat Environment

America is an open, technologically sophisticated, and complex Nation with a wide array of infrastructures that span important aspects of U.S. government, economy, and society. The majority are owned and operated by the private sector. Many others are owned and operated by regional public or quasi-public authorities or State, local, and tribal governments. The Nation's infrastructure is comprised of a vast number of highly interconnected assets, systems, and networks that present an attractive array of targets to terrorists. It is also highly vulnerable in the context of catastrophic natural disasters. The multifaceted and geographically diverse nature of this Nation's infrastructure also poses enormous challenges for assessing risk and implementing measures that would mitigate risk for all infrastructure regarding all possible terrorist attacks and catastrophic disasters. However, improvements in protection that focus on the prioritized elements of infrastructure that are nationally critical, can make it more difficult for terrorists to launch successful attacks and can lessen the impacts of any attack or catastrophic disaster that does occur.

1.3.2 The Nature of Possible Terrorist Attacks

Terrorist organizations have shown an understanding of the potential consequences of carefully planned attacks on economic, transportation, and symbolic targets both within the United States and abroad. Future terrorist attacks against CI/KR across the United States could seriously threaten national security, result in mass casualties, weaken the economy, and damage public morale and confidence. Additionally, terrorist attacks against these targets may represent an attempt by the attacker to promote the terrorist agenda or erode public confidence in American institutions.

Although a degree of uncertainty remains as to how, why, and when a particular target might be attacked, the NIPP considers a broad range of terrorist objectives, intentions, and capabilities. Based on that assessment, attacks against the Nation's CI/KR are contemplated to achieve three general types of effects:

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

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

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

1.3.3 Characteristics of Terrorism

The number of high-profile terrorist attacks that have occurred internationally and domestically in the last decade underscores the determination and resiliency of terrorist organizations. Extremist terrorist organizations that have declared war against the United States have proven to be relentless and patient, in addition to being opportunistic and flexible. They have learned from experience and modified their tactics and targets to exploit perceived vulnerabilities and avoid observed strengths. As security measures around more predictable targets increase, terrorists may shift their focus to less protected potential targets. Enhancing countermeasures for any one terrorist tactic or target, therefore, makes it more likely that terrorists will favor another. Although information about possible terrorist targets is incomplete, the current analysis of terrorist goals and motivations point to possible strikes against the Nation's CI/KR.

1.4 All-Hazards and CI/KR Protection

Owners and operators, government emergency managers, and first-responders have developed strategies, plans, policies, and procedures for preparing for, mitigating, responding to, and recovering from a full spectrum of natural and man-made hazards that make a significant contribution to the overall CI/KR protection effort. These efforts are complementary to the NIPP framework, which is aimed at enhancing the protection of America's CI/KR from terrorist attacks. In fact, the day-to-day public-private sector coordination structures that govern the NIPP and those that govern incident management under the National Response Plan (NRP) are one and the same. The NIPP and other all-hazards plans and initiatives work together to help make the Nation safer, more secure, and more resilient. As a result, the NIPP, and the public and private sector partnership that it represents, provides a stronger foundation for the broader set of protection and preparedness efforts that address the entire range of potential hazards. These NIPP elements include:

- A comprehensive approach that integrates authorities, capabilities, and resources on a national, regional, and local scale;

- A complete and accurate assessment of the Nation's CI/KR that not only prioritizes protection efforts, but also enables response and recovery efforts;
- An organization and coordinating structure to enable effective partnership with State, local, and tribal governments and regional public-private partnerships, as well as the private sector;
- An integrated approach to enhancing protection of the physical, cyber, and human elements of the Nation's CI/KR in which physical and cyber measures complement one another; and
- The development and use of sophisticated analytical and modeling tools to help develop and emphasize effective protective solutions in an all-hazards context.

1.5 The Secretary of Homeland Security's Role in CI/KR Protection

Protection of the Nation's CI/KR is one of six critical mission areas assigned to DHS in the Homeland Security Act of 2002. The National Strategy for Homeland Security established the national CI/KR vision with a charge to "forge an unprecedented level of cooperation throughout all levels of government, with private industry and institutions, and with the American people to protect our critical infrastructures and key assets from terrorist attack."⁴ The National Strategy also established the need for a national infrastructure protection plan as the primary vehicle to organize the complementary efforts of government and private institutions to raise security over the long term to levels appropriate to each target's criticality, vulnerability, and threat.

HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection, provided the direction to implement this vision and mandated development of the NIPP. In HSPD-7, the President designated the Secretary of Homeland Security as the "principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructures and key resources." In this capacity, the Secretary of Homeland Security is responsible for coordinating and implementing the development of the NIPP with participation from a wide range of government and private sector security partners. This responsibility includes addressing the complexities of the Nation's Federal system of government, and its multifaceted and interdependent economy, as well as the need for close cooperation between the private sector and government at all levels to initiate and sustain effective protective programs.

1.6 Goal and Objectives of the NIPP

The overarching goal of the NIPP is to:

Enhance protection of the Nation's CI/KR in order to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and

⁴ The National Strategy for Homeland Security uses the term "key assets," defined as individual targets whose destruction would not endanger vital systems, but could create local disaster or profoundly damage our Nation's morale or confidence. The Homeland Security Act of 2002 and HSPD-7 use the term "key resources," defined more generally to capture publicly or privately controlled resources essential to the minimal operations of the economy or government. "Key resources" is the current terminology.

1 *enable national preparedness, timely response, and rapid recovery in the event of an*
2 *attack, natural disaster, or other emergency.*

3 Achieving this goal requires meeting three principal objectives:

- 4 • Build security partnerships to implement CI/KR protection programs;
- 5 • Implement a long-term risk-reduction program; and
- 6 • Maximize efficient use of resources for CI/KR protection.

7 **1.6.1 Building Security Partnerships**

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

- 10 • Exchange ideas, approaches, and best practices;
- 11 • Facilitate security planning and resource allocation;
- 12 • Establish effective coordinating structures and information-sharing processes and protocols among
13 security partners;
- 14 • Enhance coordination with the international community; and
- 15 • Build public awareness.

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

19 **1.6.2 Implementing a Long-Term CI/KR Risk-Reduction Program**

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

- 21 • Establish a risk management framework to guide CI/KR protection programs;
- 22 • Provide intelligence and information to SSAs for sharing with the CI/KR sector partners as permitted by
23 law;
- 24 • Identify and regularly update the status of CI/KR protection programs within and across sectors;
- 25 • Conduct and update risk assessments at the asset, sector, cross-sector, and transnational levels;
- 26 • Analyze, warehouse, and share risk assessment data consistent with relevant legal requirements and
27 information protection responsibilities;
- 28 • Develop and deploy new technologies to enable more effective and efficient CI/KR protection; and
- 29 • Provide a system for continuous measurement and improvement of CI/KR protection, including:
 - 30 ➤ Establishing performance metrics to assess the effectiveness of protective programs; and
 - 31 ➤ Updating of the NIPP and SSPs as required.

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

1.6.3 Maximizing Efficient Use of Resources for CI/KR Protection

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

- Supports prioritization of protective actions within and across sectors;
- Informs the annual Federal process regarding planning, programming, and budgeting for national-level protection activities; and
- Helps to align the resources of the Federal budget to the CI/KR protection mission.
- Takes into account State and local government and private sector considerations related to planning, programming, and budgeting;
- Identifies potential incentives for security-related activities where they do not naturally exist in the marketplace;
- Draws on expertise across organizational and national boundaries;
- Shares expertise and speeds implementation of best practices; and
- Recognizes the need to build a business case for private sector CI/KR investments.

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

1.7 Planning Assumptions

The NIPP is based on the following planning assumptions that relate to the sector-specific nature of protective measures, adaptive nature of the threat, and all-hazards requirement inherent in CI/KR protection.

Sector-Specific Nature of CI/KR Protection

- Approaches to CI/KR protection and risk management vary based on sector characteristics, requirements, and maturity;
- Assets, systems, and networks vary in criticality from and within one CI/KR sector to another;

- Many assets, systems, and networks depend on multiple elements and networks at the Federal, State, and local levels. In some cases, a failure in one sector will significantly impact another sector's ability to perform necessary and critical functions;
- Successful CI/KR protection requires robust baseline information on assets, systems, and networks within and across CI/KR sectors, regions⁵, and specific localities;
- Owners and operators conduct risk management planning and invest in security from a business perspective.
- In some sectors, private sector firms own the vast majority of CI/KR; and
- Strong relationships among security partners are essential to meet the CI/KR protection goals set forth in the NIPP.

Adaptive Nature of the Terrorist Threat

- CI/KR protection activities take place in a highly dynamic threat environment. The general threat environment changes as the capabilities and the intentions of terrorists evolve;
- It is not practical to protect all assets, systems, and networks against every possible terrorist attack. A risk-based approach driven by intelligence analysis and reporting is crucial to an effective risk management strategy and efficient resource allocation;
- Given the uncertain nature of the terrorist threat, the full range of threats, not just the most likely or those involving the most frequent reporting, must be regarded when considering actions to enhance CI/KR protection; and
- A proactive approach is required to enhance decision-making processes, provide advance warning to potentially targeted CI/KR, and assist CI/KR owners and operators in taking protective steps to enhance protection of CI/KR against terrorist attacks.

All-Hazards Nature of CI/KR Protection

- Natural disasters such as floods, hurricanes, tornadoes, wildfires, pandemics, and earthquakes, and unintentional man-made hazards, such as oil spills or nuclear power plant accidents, also pose a threat to the Nation's CI/KR; and
- Efforts to enhance the protection of CI/KR from terrorist attacks also support all-hazards preparedness and response in most instances.

1.8 Special Considerations

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

⁵ An area with shared geography, economies, or other characteristics that can serve as the focal point for infrastructure protection through public and private partnerships.

Protection of Sensitive Infrastructure Information

- Partnership with the private sector requires the establishment of mutually beneficial, trusted relationships supported by a network approach to providing access to information;
- Great care must be taken by the government to ensure that sensitive infrastructure information is protected and used appropriately in enhancing the protection of the Nation's CI/KR;
- Information on specific industry assets and vulnerabilities is particularly sensitive because public release may lead to breaches in security, competitive advantage, and/or adverse impacts on an industry's position in the marketplace; and
- DHS does not have the statutory authority to direct industry to share data or information.

Protection of sensitive infrastructure information involves two activities:

- **Protection** from unauthorized public disclosure; and
- **Security** to guard against damage, theft, or exploitation (e.g., firewalls, physical security).

The Cyber Dimension

- The U.S. economy and national security are highly dependent upon the cyber infrastructure. Cyber infrastructure enables all sectors' functions and services, resulting in a highly interconnected and interdependent network of CI/KR;
- A spectrum of malicious actors could conduct attacks against the cyber infrastructure using easily available cyber attack tools. Because of the interconnected nature of the cyber infrastructure, these attacks could spread quickly and have a debilitating impact;
- The use of innovative technology and interconnected networks in operations improves productivity and efficiency, but also increases the Nation's risk of cyber threats if cybersecurity is not addressed and integrated appropriately;
- The interconnected and interdependent nature of the Nation's CI/KR makes it problematic to address the protection of physical and cyber assets independently; and
- The NIPP addresses reducing cyber risk and enhancing cybersecurity in two ways: (1) as a cross-sector cyber element that involves both DHS and the SSAs, and (2) as a major component of the Information Technology (IT) Sector's responsibility.

Cybersecurity includes two active measures:

Prevention of

- damage to,
- unauthorized use of, and
- exploitation of,

and restoration of

- electronic information and communications systems, and
- the information contained therein

to ensure the confidentiality, integrity, and availability of electronic information.

Cyber infrastructure includes electronic information and communications systems and the information contained in those systems.

Information and communications systems are comprised of all the hardware and software that process, store, or communicate information; this includes Supervisory Control and Data Acquisition (SCADA) systems.

The Human Element

- The NIPP recognizes that each CI/KR asset, system, and network is made of component physical, cyber, and human elements;
- The human element requires:
 - Identifying and preventing the insider threat resulting from infiltration or individual employees determined to do harm; and
 - Identifying and protecting employees and other persons with critical knowledge or functions from terrorist attack;
- Assessing human element vulnerabilities is more subjective than assessing the physical vulnerabilities of corresponding assets, systems, and networks; and
- Diverse protective programs and actions to address threats posed by employees and to employees need to be put into place across the country.

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

Physical – tangible property;

Cyber – electronic information and communications systems, and the information contained therein, and

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

International CI/KR Protection

- The NIPP addresses international CI/KR protection, including interdependencies and vulnerabilities based on threats that originate outside the country.
- The U.S. government works with foreign governments and international/multinational organizations to enhance the confidentiality, integrity, and availability of cyber infrastructures and products.
- Protection of physical assets located on or near the borders with Canada and Mexico, or relied upon jointly with the United States, require coordination with, and planning and/or sharing resources among, neighboring countries.
- The U.S. government and American corporations have a significant number of facilities located outside of the United States that may be considered CI/KR.
- Special consideration is required when infrastructure is extensively integrated into an international or global market (e.g., financial services, agriculture, energy, transportation, or information technology) or when a sector relies on inputs that are not within the control of U.S. entities.

2. Authorities, Roles, and Responsibilities

The kind of true partnership that protecting the homeland requires means that we not only share information but also responsibility. It means that we not only exchange expertise but also expect accountability. It means that our partners must bear a part of the security burden as well as become part of the security solution.

*Michael Chertoff
Secretary
U.S. Department of Homeland Security*

Improving the protection of the Nation's CI/KR in an all-hazards environment requires a comprehensive, unifying organization, clearly defined roles and responsibilities, and close cooperation across all levels of government and the private sector. Protection authorities, requirements, resources, capacities, and risk landscapes vary widely across governmental jurisdictions, sectors, and individual industries and enterprises. This reality presents a complex set of challenges in terms of NIPP compliance and performance measurement. Hence, successful implementation of the NIPP and supporting SSPs depends on an effective partnership framework that fosters integrated, collaborative engagement and interaction; establishes a clear division of labor among diverse security partners; and efficiently allocates the Nation's protection resources based on risk and need.

This Chapter includes a brief overview of the relevant authorities and outlines the principal roles and responsibilities of DHS; SSAs; other Federal departments and agencies; State, local, and tribal jurisdictions; private sector owners and operators; and other security partners who share responsibility in protecting the Nation's CI/KR under the NIPP. A comprehensive and unequivocal understanding of these roles and responsibilities provides the foundation for an effective and sustainable national protection effort.

2.1 Authorities

The roles and responsibilities described in this Chapter are derived from a series of authorities, including the Homeland Security Act of 2002, other CI/KR protection-related legislation, Executive Orders, Homeland Security Presidential Directives, and Presidential strategies. More detailed information on authorities is included in Appendix 1.

The Homeland Security Act of 2002 provides the primary authority for the overall homeland security mission and outlines DHS responsibilities in the protection of the Nation's CI/KR. It established the DHS mission, including "reducing the Nation's vulnerability to terrorist attacks" and charged the department with the responsibility of evaluating vulnerabilities and ensuring that steps are implemented to protect the high-risk elements of America's CI/KR, including food and water systems, agriculture, health systems and emergency services, information technology and telecommunications, banking and finance, energy (electrical, nuclear, gas and oil, dams), transportation (air, road, rail, ports, waterways), the chemical and defense industries, postal and shipping entities, and national monuments and icons. Title II, Section 201, of the Act assigned primary responsibility to DHS to develop a comprehensive national plan for securing CI/KR and for recommending "the measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other agencies of the Federal government and in

cooperation with State and local government agencies and authorities, the private sector, and other entities."

A number of other statutes provide authorities both for cross-sector and sector-specific CI/KR protection and security efforts. Some examples of other CI/KR protection-related legislation include: The Public Health Security and Bioterrorism Preparedness and Response Act of 2002, which was intended to improve the ability of the United States to prevent, prepare for, and respond to acts of bioterrorism and other public health emergencies; the Resource Conservation and Recovery Act of 1976, giving the Environmental Protection Agency (EPA) the responsibility to control hazardous waste from "cradle to grave"; the Oil Pollution Act of 1990; the Maritime Transportation Security Act; the Energy Policy and Conservation Act; the Critical Infrastructure Information Act; the Federal Information Security Act; and others.

These separate authorities are tied together as part of the national approach for CI/KR protection through the unifying framework established in HSPD-7. HSPD-7, issued in December 2003, established the U.S. policy for "enhancing protection of the Nation's CI/KR." The following sections address the security partner roles and responsibilities under this integrated approach.

2.2 Roles and Responsibilities

Given the fact that terrorist incidents and certain natural or man-made disasters can have national-level impact, it is incumbent upon the Federal government to provide overarching leadership and coordination in the CI/KR protection mission area.

2.2.1 Department of Homeland Security

Under the HSPD-7 framework, DHS is responsible for leading, integrating, and coordinating the overall national effort to enhance CI/KR protection, including developing the NIPP and supporting SSPs; developing and implementing comprehensive multi-tiered risk-reduction programs and methodologies; developing cross-sector and cross-jurisdictional protection guidance, guidelines, and protocols; and establishing risk management and performance criteria and metrics within and across sectors. In addition to these overarching leadership and cross-sector responsibilities, DHS serves as the SSA for 10 of the CI/KR sectors identified in HSPD-7: information technology; telecommunications; transportation; chemicals; emergency services; commercial nuclear reactors, material, and waste; postal and shipping; dams; government facilities; and commercial facilities. Specific SSA responsibilities are discussed in Section 2.2.

Consistent with the NIPP framework, additional overarching DHS CI/KR protection roles and responsibilities include the following:

- Identifying, prioritizing, and coordinating the protection of national-level CI/KR, with a particular focus on CI/KR that could be exploited to cause catastrophic health effects or mass casualties comparable to those produced by a weapon of mass destruction;
- Managing the overall process for building security partnerships and leveraging sector-specific security expertise, relationships, and resources across CI/KR sectors, including oversight and support of the sector partnership model described in Chapter 4, and collaborating with foreign countries and international organizations to strengthen the protection of U.S. CI/KR;

- 1 • Establishing and maintaining a comprehensive, multi-tiered, dynamic information-sharing network
2 designed to provide timely and actionable threat information, assessments, and warnings to public and
3 private sector security partners. This responsibility includes protecting information voluntarily provided
4 by the private sector and facilitating the development of sector-specific and cross-sector information-
5 sharing and analysis systems, mechanisms, and processes;
- 6 • Integrating and analyzing law enforcement, intelligence, and other information in order to identify and
7 assess the nature and scope of terrorist threats to CI/KR – including precursors and indicators of an
8 attack – and understand those threats in terms of CI/KR vulnerabilities;
- 9 • Managing comprehensive risk assessment programs for high-risk CI/KR, identifying protection priorities
10 across sectors and jurisdictions, and incorporating CI/KR protective programs as a key component of
11 the all-hazards approach to domestic incident management;
- 12 • Facilitating the sharing of CI/KR protection best practices and processes, and risk assessment
13 methodologies and tools across sectors and jurisdictions;
- 14 • Sponsoring CI/KR protection-related research and development (R&D), demonstration projects, and
15 pilot programs;
- 16 • Seeding development and transfer of advanced technologies while leveraging private sector expertise
17 and competencies, as appropriate;
- 18 • Promoting national-level CI/KR protection education, training, and awareness;
- 19 • Conducting analysis of cross-sector dependencies and interdependencies, to include cyber
20 considerations;
- 21 • Conducting modeling and simulation activities to enable national- and sector-level risk comparisons;
- 22 • Informing the annual Federal budget process based on CI/KR risk and need in coordination with SSAs
23 and other security partners;
- 24 • Monitoring performance measures for the national CI/KR protection program and NIPP implementation
25 process to enable continuous improvement, and reporting progress and critical gaps to the Executive
26 Office of the President (EOP);
- 27 • Integrating national efforts for the protection and recovery of critical information systems and cyber
28 components of physical CI/KR, including analysis, warning, information-sharing, vulnerability reduction,
29 and mitigation activities and programs;
- 30 • Evaluating preparedness for CI/KR protection across sectors and jurisdictions through the National
31 Exercise Program;
- 32 • Working with the Department of State, SSAs, and other security partners to ensure that U.S. CI/KR
33 protection efforts are fully coordinated with international partners; and
- 34 • Evaluating the need for and coordinating the protection of additional CI/KR categories over time, as
35 appropriate.

2.2.2 Sector-Specific Agencies

Recognizing that each CI/KR sector possesses its own unique characteristics, operating models, and risk landscape, HSPD-7 designates Federal government SSAs for each of the 17 CI/KR sectors (see Table 2-1). At the sector level, SSAs are responsible for working with DHS to implement the NIPP sector partnership model and risk management framework, develop protective programs and related requirements, and provide CI/KR protection guidance in line with the overarching guidance established by DHS pursuant to HSPD-7. Working in collaboration with security partners, they are responsible for developing and submitting SSPs and sector-level performance feedback to DHS to enable national-level gap assessments.

Table 2-1: Sector-Specific Agencies and HSPD-7 Assigned CI/KR Sectors

Department of Agriculture Agriculture, food (meat, poultry, egg products)	Department of the Interior National monuments and icons
Department of Health and Human Services Public health and healthcare	Department of Defense Defense industrial base
Food (other than meat, poultry, egg products)	Department of Homeland Security Chemical (DHS/IP)
Environmental Protection Agency Drinking water and wastewater treatment systems	Commercial facilities (DHS/IP)
Department of Energy Energy, including the production, refining, storage, and distribution of oil and gas, and electric power (except for commercial nuclear power facilities)	Dams (DHS/IP)
Department of the Treasury Banking and finance	Emergency services (DHS/IP)
	Commercial nuclear reactors, materials, and waste (DHS/IP)
	Information technology (DHS/Cyber and Telecommunications Security)
	Telecommunications (DHS/Cyber and Telecommunications Security)
	Postal and shipping (DHS/TSA)
	Transportation systems (DHS/TSA, USCG ⁶)
	Government facilities (DHS/FPS)

In accordance with HSPD-7, SSAs are also responsible for collaborating with the private sector security partners and encouraging the development of appropriate information-sharing and analysis mechanisms within the sector. They also are responsible for supporting sector coordinating mechanisms to facilitate sharing of information on physical and cyber threats, vulnerabilities, incidents, recommended protective measures, and security-related best practices. This includes encouraging voluntary security-related information sharing among private entities within the sector, as well as among public and private entities.

SSAs perform the activities above, as appropriate and consistent with existing authorities (including regulatory authorities in some instances), in close cooperation with other security partners. In order to achieve effective and efficient implementation of the NIPP and supporting SSPs, SSAs also identify and

⁶ USCG is the lead agency for the maritime transportation mode.

1 prioritize CI/KR protection requirements and address the associated funding in their individual annual
2 budget submissions. SSAs are responsible for outlining these sector-specific CI/KR protection
3 requirements and related budget projections as a component of their required annual report to DHS.

4 Additional SSA responsibilities include the following:

- 5 • Identifying, prioritizing, and coordinating the protection of sector-level CI/KR, with a particular focus on
6 CI/KR that could be exploited to cause catastrophic health effects or mass casualties comparable to
7 those produced by a weapon of mass destruction;
- 8 • Managing the overall process for building security partnerships and leveraging CI/KR security
9 expertise, relationships, and resources within the sector, including sector-level oversight and support of
10 the sector partnership model described in Chapter 4;
- 11 • Managing comprehensive risk assessment/management programs for high-risk CI/KR, identifying
12 protection priorities, and incorporating CI/KR protection activities as a key component of the all-hazards
13 approach to domestic incident management within the sector;
- 14 • Facilitating the sharing of CI/KR protection best practices and processes, and risk assessment
15 methodologies and tools within the sector;
- 16 • Promoting sector-level CI/KR protection education, training, and awareness;
- 17 • Identifying CI/KR dependencies and interdependencies within the sector;
- 18 • Informing the annual Federal budget process based on risk and need in coordination with security
19 partners;
- 20 • Monitoring performance measures for sector-level CI/KR protection and NIPP implementation process
21 to enable continuous improvement, and reporting progress and gaps to DHS;
- 22 • Contributing to the annual National Critical Infrastructure Protection R&D Plan;
- 23 • Supporting DHS-initiated data calls to populate the National Asset Database (NADB), enable national-
24 level risk assessment, and inform national-level resource allocation;
- 25 • Working with DHS to develop, evaluate, or validate sector-specific risk assessment tools;
- 26 • Supporting sector-level interdependency, consequence, and other analysis as required;
- 27 • Coordinating sector-level participation in the National Exercise Program and other sector-level
28 preparedness activities;
- 29 • Assisting sector security partners in their efforts to:
 - 30 ➤ Organize and conduct protection and continuity-of-operations planning, and elevate awareness
31 and understanding of threats and vulnerabilities to their assets, systems, and networks; and
 - 32 ➤ Identify and promote effective sector-specific protection practices and methodologies;
- 33 • Allocating resources for CI/KR protection based on risk and need;
- 34 • Understanding and mitigating sector-specific cyber risk by developing appropriate protective measures,
35 information-sharing mechanisms, and emergency recovery plans for cyber assets, systems, and
36 networks within the sector; and

- Supporting DHS and the Department of State in efforts to integrate U.S. CI/KR protection programs into the international and global markets, and address relevant dependency, interdependency, and cross-border issues.

2.2.3 Other Federal Departments, Agencies, and Offices

All Federal departments and agencies function as security partners in coordination with DHS and the SSAs. In accordance with HSPD-7, they are required to cooperate with DHS in implementing CI/KR protection efforts, consistent with the Homeland Security Act and other applicable legal authorities. In this capacity, they support implementation of the NIPP and SSPs, as appropriate, and are responsible for identification, prioritization, assessment, remediation, and enhancing protection of CI/KR under their control. HSPD-7 also requires that all departments and agencies work with the sectors relevant to their responsibilities to reduce the consequences of catastrophic failures not caused by acts of terrorism.

Federal departments and agencies that are not designated as SSAs, but that have unique responsibilities, functionality, or expertise in a particular CI/KR sector, will:

- Assist in assessing risk, prioritizing CI/KR, and enabling protective actions and programs within that sector;
- Play a role as the regulatory agency for owners and operators represented within that sector when so designated by statute; and
- Collaborate with all relevant security partners to share security-related information within the sector, as appropriate.

Depending on their regulatory roles and their relationships with the SSAs, these agencies may play a supporting role in developing and implementing SSPs and implementing related protective activities within the sector.

Under HSPD-7, a number of Federal departments and agencies and components of the EOP have special functions related to CI/KR protection. These include:

- **The Department of State**, in coordination with DHS and the departments of Justice, Commerce, Defense, and Treasury, works with foreign countries and international organizations to strengthen U.S. CI/KR protection efforts.
- **The Department of Justice**, including the Federal Bureau of Investigation (FBI), acts to reduce domestic terrorist threats, and investigates and prosecutes actual or attempted attacks on, sabotage of, or disruptions of CI/KR.
- **The Department of Commerce** works with DHS and private sector, research, academic, and other government organizations to improve cybersecurity and technology related to CI/KR protection, including using its authority under the Defense Production Act to ensure the timely availability of industrial products, materials, and services to meet homeland security requirements;
- **The Department of Transportation** collaborates with DHS on all matters related to transportation security and transportation infrastructure protection, and is additionally responsible for operating the

1 National Airspace System (NAS). The Department of Transportation and DHS collaborate on regulating
2 the transportation of hazardous materials by all modes (including pipelines);

- 3 • **The Nuclear Regulatory Commission** works with DHS and the Department of Energy, as
4 appropriate, to ensure the necessary protection of commercial nuclear reactors for generating electric
5 power and non-power nuclear reactors used for research, testing, and training; nuclear materials in
6 medical, industrial, and academic settings and facilities that fabricate nuclear fuel; and the
7 transportation, storage, and disposal of nuclear materials and waste;
- 8 • **The Intelligence Community, the Department of Defense, Department of the Interior,** and other
9 appropriate Federal agencies collaborate with DHS to develop the geospatial program mandated by
10 HSPD-7. This program will map, image, analyze, and sort CI/KR using commercial satellite and
11 airborne systems, as well as existing agency capabilities;
- 12 • **The Office of Science and Technology Policy** coordinates with DHS to further interagency R&D
13 related to CI/KR protection; and
- 14 • **The Office of Management and Budget** oversees the implementation of government-wide policies,
15 principles, standards, and guidelines for Federal government computer security programs.

16 2.2.4 State, Territorial, Local, and Tribal Governments

17 State, Territorial, local, and tribal governments are responsible for implementing the homeland security
18 mission, protecting public safety and welfare, and ensuring the provision of essential services to
19 communities and industries within their jurisdictions. They also play a very important and direct role in
20 enabling the protection of the Nation's CI/KR, including CI/KR under their control, as well as CI/KR owned
21 and operated by other NIPP security partners resident within their jurisdictions. The efforts of these public
22 entities are critical to the effective implementation of the NIPP, SSPs, and various jurisdictionally focused
23 protection plans. They are equally critical in terms of enabling time-sensitive, post-event CI/KR response,
24 restoration, and recovery activities.

25 Security partners at all levels of government recently developed homeland security strategies that align with
26 and support the overarching priorities established in the National Preparedness Goal. With the inclusion of
27 NIPP implementation as one of these overarching national priorities, CI/KR protection programs form an
28 essential component of State, Territorial, local, and tribal homeland security strategies, particularly with
29 regard to informing funding priorities and security investment decisions. To permit effective NIPP
30 implementation and use of performance measurement at each jurisdictional level, these protection
31 programs should reference all core elements of the NIPP framework, including key cross-jurisdictional
32 security and information-sharing linkages, as well as specific CI/KR protective programs focused on risk
33 reduction. These programs should also support DHS and SSA efforts to identify, ensure connectivity with,
34 and enable the protection of CI/KR of national-level criticality within the jurisdiction.

35 2.2.4.1 State and Territorial Governments

36 State and Territorial governments are responsible for establishing security partnerships, facilitating
37 coordinated information sharing, and enabling planning and preparedness for CI/KR protection within their
38 jurisdictions. They serve as crucial coordination hubs, bringing together prevention, protection,
39 preparedness, and response authorities; capacities; and resources among local jurisdictions, across

1 sectors, and between regional entities. States and Territories also act as conduits for requests for Federal
2 assistance when the threat situation or current incident exceeds the capabilities of public and private sector
3 security partners at lower jurisdictional levels.

4 State and Territorial governments are responsible for developing and implementing statewide/regional
5 CI/KR protection programs that reflect the full range of NIPP-related activities. State/Territorial programs
6 should address all relevant aspects of CI/KR protection, leverage support from homeland security
7 assistance programs that apply across the homeland security mission area, and reflect priority activities in
8 their strategies to ensure that resources are effectively allocated. Effective statewide and regional CI/KR
9 protection efforts should be integrated into the overarching homeland security program framework at the
10 State level to ensure that prevention, protection, response, and recovery efforts are synchronized and
11 mutually supportive. CI/KR protection at the State/Territorial level must cut across all sectors present within
12 the State and support national, State, and local priorities. The program also should explicitly address the
13 unique geographical issues, including trans-border concerns, as well as interdependencies among sectors
14 and jurisdictions within those geographical boundaries.

15 Specific CI/KR protection-related activities include:

- 16 • Acting as a focal point for and promoting the coordination of protective and emergency response
17 activities, preparedness programs, and resource support among local jurisdictions and regional
18 partners;
- 19 • Developing a unified approach to CI/KR identification, risk determination, mitigation planning, and
20 prioritized security investment, and exercising preparedness among all relevant stakeholders within
21 their jurisdictions;
- 22 • Acting as conduits for requests for Federal assistance when the threat or current situation exceeds the
23 capabilities of State and local jurisdictions and private entities resident within them;
- 24 • Facilitating the exchange of security information – including threat assessments, attack indications and
25 warnings, and advisories – within and across jurisdictions and sectors therein;
- 26 • Participating in NIPP sector partnership model, including Government Coordinating Councils (GCCs),
27 Sector Coordinating Councils (SCCs), and other CI/KR governance efforts relevant to the given
28 jurisdiction;
- 29 • Ensuring that funding priorities are addressed and that resources are allocated efficiently and
30 effectively to achieve the CI/KR protection mission in accordance with relevant plans and strategies;
- 31 • Providing information on CI/KR deemed critical from national, State, regional, local, and/or tribal
32 perspectives to enable prioritized protection and restoration of critical public services, facilities, utilities,
33 and processes within the jurisdiction;
- 34 • Addressing unique geographical issues, including trans-border concerns, dependencies, and
35 interdependencies among the sectors within the jurisdiction;
- 36 • Identifying and implementing cross-sector protective actions within the jurisdiction corresponding to
37 each level of the Homeland Security Advisory System;
- 38 • Establishing cybersecurity programs and associated awareness training within the jurisdiction;

- Documenting lessons learned from pre-disaster mitigation efforts, exercises, and actual incidents and applying that learning, where applicable, to the CI/KR protection context;
- Identifying and communicating requirements for CI/KR-related R&D to DHS; and
- Providing annual reports to DHS on CI/KR protection program implementation and progress.

2.2.4.2 Local Governments

Local governments represent the tip of the spear of homeland security and, more specifically, CI/KR protection in the context of the NIPP partnership model. They also are the “face” of numerous critical public services and functions, as well as public confidence in government. In terms of the CI/KR protection mission, most disruptions or malevolent acts begin as a local situation. Regardless of who owns or operates the affected asset, system, or network, local authorities typically must shoulder the weight of initial prevention, response, and recovery operations until coordinated support from other sources becomes available. In these terms, local governments are critical partners under the NIPP framework. They drive the emergency preparedness of the communities they serve, as well as local participation in NIPP and SSP implementation across a variety of local jurisdictional security partners, including government agencies, businesses, and private citizens.

In addition to the responsibilities outlined above, the CI/KR protection focus at the local level should include:

- Acting as a focal point for and promoting the coordination of protective and emergency response activities, preparedness programs, and resource support among local agencies, businesses, and citizens;
- Developing a unified approach to CI/KR identification, risk determination, mitigation planning, and prioritized security investment, and exercising preparedness among all relevant security partners within the jurisdiction;
- Facilitating the exchange of security information – including threat assessments, attack indications and warnings, and advisories – among security partners within the jurisdiction;
- Participating in NIPP sector partnership model, including GCCs, SCCs, and other CI/KR governance efforts relevant to the given jurisdiction;
- Ensuring that funding priorities are addressed and that resources are allocated efficiently and effectively to achieve the CI/KR protection mission in accordance with relevant plans and strategies;
- Providing information on CI/KR deemed critical from the local perspective to enable prioritized protection and restoration of critical public services, facilities, utilities, and processes within the jurisdiction;
- Addressing unique geographical issues, including trans-border concerns, dependencies, and interdependencies among agencies and enterprises within the jurisdiction;
- Identifying and implementing cross-sector protective actions within the jurisdiction corresponding to each level of the Homeland Security Advisory System;
- Establishing cybersecurity programs and associated awareness training within the jurisdiction;

- Documenting lessons learned from pre-disaster mitigation efforts, exercises, and actual incidents, and applying that learning, where applicable, to the CI/KR protection context; and
- Conducting CI/KR protection public awareness activities.

2.2.4.3 Tribal Governments

To a great extent, tribal government roles and responsibilities regarding CI/KR protection mirror those of State and local governments as detailed above. Tribal governments are ultimately accountable for the public health, welfare, and safety of tribal members, as well as the protection of CI/KR and continuity of essential services under their jurisdiction. As a partner under the NIPP partnership model, tribal governments must ensure close coordination with Federal, State, and local government counterparts to achieve synergy in the implementation of the NIPP and SSP frameworks within their jurisdictions. This is particularly important in the context of information sharing, risk analysis and management, awareness, preparedness planning, protective program investments and initiatives, and resource allocation. To facilitate this interaction, tribal governments should be active participants in the NIPP governance structures detailed in Chapter 4.

2.2.4.4 Regional Partners

Regional security partnerships include a variety of public-private sector initiatives that cross jurisdictional and/or sector boundaries and focus on homeland security preparedness, protection, response, and recovery within or serving the population of a defined geographical area. Specific regional initiatives range in scope from organizations that include multiple jurisdictions and industry partners within a single State to groups that involve jurisdictions and enterprises in more than one State and across international borders. In many cases, State governments also collaborate through the adoption of interstate compacts to formalize regionally based partnerships regarding CI/KR protection.

Security partners leading or participating in regional initiatives are encouraged to capitalize on the larger area- and sector-specific expertise and relationships to:

- Promote collaboration among security partners in implementing NIPP-related CI/KR risk assessment and protection activities;
- Facilitate education and awareness of CI/KR protection efforts occurring within their geographical area;
- Coordinate regional exercise and training programs, including a focus on CI/KR interdependencies and protection collaboration across jurisdictional and sector boundaries;
- Work with State, local, and tribal governments, and the private sector to evaluate regional and cross-sector CI/KR interdependencies, to include cyber considerations;
- Conduct appropriate regional planning efforts and undertake appropriate partnership agreements to enable regional CI/KR protection activities and enhanced response to emergencies;
- Facilitate information sharing between and among regional initiative members and external partners; and
- Share information on progress and CI/KR protection requirements with DHS.

2.2.5 Private Sector and Other Owners and Operators

Owners and operators generally represent the first line of defense for the CI/KR under their control. Owners and operators are responsible for taking action to support risk management planning and investments in security as a necessary component of prudent business planning and operations. In today's risk environment, these activities generally include reassessing and adjusting continuity-of-operations and emergency management plans, building in increased resiliency and redundancy into business processes and systems, hardening facilities against physical and cyber attacks and natural disasters, and increased coordination with external organizations to avoid or minimize the impacts on surrounding communities or industry partners.

For most enterprises, the level of investment in security reflects risk vs. consequence tradeoffs that are based on two factors: (1) what is known about the risk environment, and (2) what is economically justifiable and sustainable in a competitive marketplace or in an environment of limited government resources. In the context of the first factor, the Federal government is uniquely postured to help inform critical security investment decisions and operational planning. For example, owners and operators generally look to the public sector as a primary source of security-related best practices and threat information, including attack indications and warnings and sector-level threat assessments. In relationship to the second factor, owners and operators also generally rely on government entities to address risks outside of their property or in situations in which the current threat exceeds an enterprise's capability to protect itself beyond a reasonable level of additional investment. In this situation, public and private sector security partners at all levels must collaborate with one another to address the protection of national-level CI/KR, provide timely warning, and promote an environment in which the private sector can better carry out its specific protection responsibilities.

The CI/KR protection responsibilities of specific owners or operators vary widely within and across sectors. Some sectors have regulatory or statutory frameworks that govern private sector security operations within the sector; however, most are guided by voluntary security regimes or adherence to industry-promoted best practices. Within this diverse protective landscape, private sector entities can better secure the CI/KR under their control by:

- Performing comprehensive risk assessments tailored to their specific sector, enterprise, or facility risk landscape;
- Developing an awareness of critical dependencies and interdependencies at the sector, enterprise, and facility level;
- Implementing protective actions and programs to reduce identified vulnerabilities appropriate to the level of risk presented;
- Developing and coordinating CI/KR protective and emergency response actions, plans, and programs with appropriate Federal, State, and local government authorities;
- Participating in the NIPP sector partnership model, (including SCCs and information-sharing mechanisms), as appropriate;
- Assisting and supporting Federal, State, and local government CI/KR protection efforts, as appropriate;

- Participating in Federal, State, and local government emergency management programs and coordinating structures;
- Adhering to recognized standards and industry best practices, including those with a cybersecurity nexus;
- Establishing resilient, robust, and/or redundant operational systems or capabilities associated with critical functions where appropriate;
- Promoting CI/KR protection education, training, and awareness programs;
- Adopting and implementing effective workforce security assurance programs to mitigate potential insider threats;
- Providing technical expertise to the SSAs and DHS when appropriate;
- Participating in regular CI/KR protection-focused exercise programs with other public and private sector security partners;
- Sharing security-related best practices and entering into operational mutual-aid agreements with other industry partners; and
- Working to identify barriers to public-private partnerships.

2.2.6 Advisory Councils

Advisory councils provide advice, recommendations, and expertise to the government regarding protection policy and activities. These entities also help enhance public-private partnerships and information sharing. They often provide an additional mechanism to engage with a pre-existing group of private sector leaders to obtain feedback on CI/KR policy and programs and make suggestions to increase the efficiency and effectiveness of government programs. Examples of CI/KR protection-related advisory councils and their associated responsibilities include:

- **Homeland Security Advisory Council (HSAC):** The HSAC provides advice and recommendations to the Secretary of Homeland Security on relevant issues. The Council members, appointed by the DHS Secretary, include experts from State and local government, public safety, security and first-responder communities, academia, and the private sector.
 - **Private Sector Senior Advisory Committee (PVSAC):** The Secretary of Homeland Security established the PVSAC as a subcommittee of the HSAC to provide the HSAC with expert advice from leaders in the private sector.
- **National Infrastructure Advisory Council (NIAC):** The NIAC provides the President, through the Secretary of Homeland Security, with advice on the security of physical and cyber systems across all CI/KR sectors. The Council is composed of up to 30 members appointed by the President. Members are selected from the private sector, academia, and State and local government. The Council was established (and amended) under Executive Orders 13231, 13286, and 13385.
- **National Security Telecommunications Advisory Committee (NSTAC):** The NSTAC provides industry-based advice and expertise to the President on issues and problems related to implementing National Security and Emergency Preparedness (NS/EP) communications policy. The NSTAC is

1 comprised of up to 30 industry chief executives representing the major communications and network
2 service providers and information technology, finance, and aerospace companies. It was created under
3 Executive Order 12382.

- 4 • **President's Information Technology Advisory Committee (PITAC):** The PITAC provides the
5 President, Congress, and Federal agencies involved in information technology R&D with expert,
6 independent advice on maintaining America's preeminence in advanced information technologies,
7 including such elements of the national CI/KR as high-performance computing, large-scale networking,
8 and high-assurance software and systems design. It was created under several acts in the 1990s and
9 was recently a topic of Executive Order 13385.

10 2.2.7 Academia, Research Centers, and Think Tanks

11 The academic, research center, and think tank communities have an important role to play in enabling
12 national-level CI/KR protection and implementation of the NIPP, including:

- 13 • Establishing Centers of Excellence (university-based partnerships) to provide independent analysis of
14 CI/KR protection issues;
- 15 • Supporting the research, development, testing, evaluation, and deployment of CI/KR protection
16 technologies;
- 17 • Analyzing, developing, and sharing best practices related to CI/KR protection efforts;
- 18 • Researching and providing innovative thinking and perspective on threats and the behavioral aspects
19 of terrorism;
- 20 • Developing best practices for cyber security;
- 21 • Preparing or disseminating guidelines, courses, and descriptions of best practices for physical security
22 and cybersecurity;
- 23 • Developing and providing suitable security risk analysis and risk management courses for CI/KR
24 protection professionals; and
- 25 • Conducting research to identify new technologies and analytical methods that can be applied by
26 security partners to support NIPP efforts.

3. The Protection Program Strategy: Reducing Risk

The cornerstone of the NIPP is its risk management framework. *Risk*, in the context of the NIPP, is defined as *the potential for loss, damage, or disruption to the Nation's CI/KR resulting from destruction, incapacitation, or exploitation during some future man-made or naturally occurring event*. The NIPP risk management framework (see Figure 3-1) establishes the process for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector-specific risk that drives CI/KR-protection activities. The framework applies to the general threat environment, as well as to specific threats or incident situations.

This Chapter addresses the use of the risk management framework as part of the overall effort to ensure a steady-state of protection within and across each of the CI/KR sectors. DHS, the SSAs, and their security partners share the responsibility for overarching implementation of the risk management framework. SSAs are responsible for leading sector-specific risk-reduction programs and for ensuring that the sector-specific application of the risk management framework is addressed in their respective SSPs. DHS supports these efforts by providing guidance, tools, and analytical support to SSAs and other security partners. DHS is responsible for using the results obtained in sector-specific risk management efforts to conduct cross-sector risk analysis and management in collaboration with other security partners. This includes the assessment of dependencies, interdependencies, and cascading effects; identification of common vulnerabilities; development and sharing of common threat scenarios; development and sharing of cross-sector measures to reduce risk; and identification of specific R&D needs.

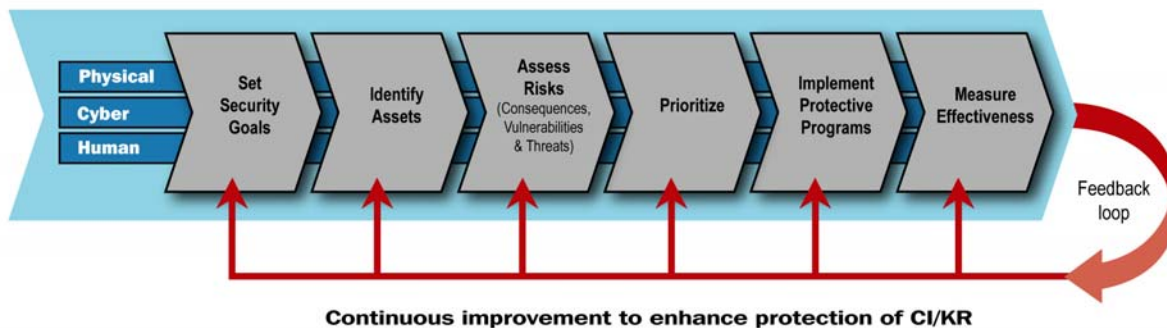


Figure 3-1: NIPP Risk Management Framework

The NIPP risk management framework includes the following activities:

- **Set security goals:** Define specific outcomes, conditions, end points, or performance targets that collectively constitute an effective protective posture.
- **Identify assets:** Develop an inventory of the assets, systems, and networks, including those located outside the United States, that make up the Nation's CI/KR, and collect information pertinent to risk management.
- **Assess risks:** Determine risk by combining potential direct and indirect consequences of a terrorist attack or other hazards (including dependencies and interdependencies associated with each identified

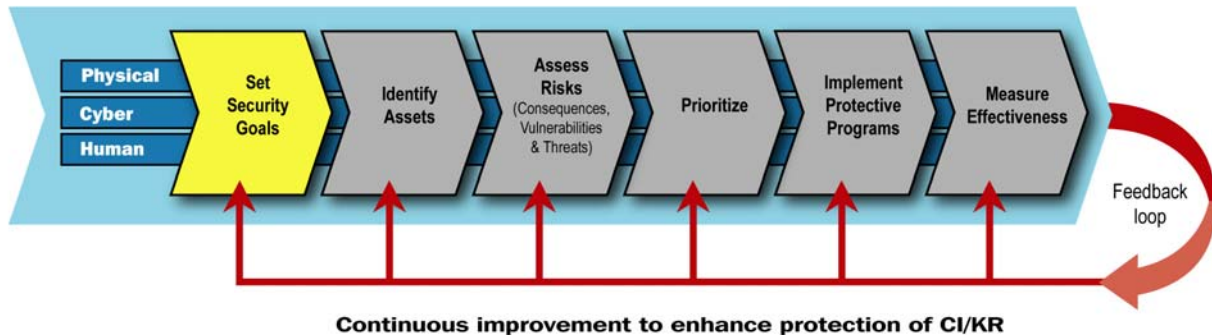
asset, system, or network), known vulnerabilities to various potential attack vectors, and general or specific threat information.

- **Prioritize:** Aggregate and analyze assessment results to determine assets, system, and network criticality and present a comprehensive picture of national CI/KR risk in order to establish protection priorities and provide the basis for protection planning and the informed allocation of resources.
- **Implement protective programs:** Select appropriate protective actions or programs to reduce the risk identified and secure the resources needed to address priorities.
- **Measure effectiveness:** Use metrics and other evaluation procedures at the national and sector levels to measure progress and assess the effectiveness of the national CI/KR protection program.

DHS uses information from metrics and other evaluation tools to support a constant feedback loop. This process allows the Federal government and its security partners to continuously improve national CI/KR protection and take actions to achieve NIPP goals and objectives as described in Chapter 1.

The physical, cyber, and human elements of CI/KR are considered during each step of the risk management framework. In addition, the sector partnership model discussed in Chapter 4 provides the structure for overarching coordination and management activities that provide the foundation for effective implementation of risk management activities for current and future CI/KR protection.

3.1 Set Security Goals



Achieving a secure, protected, and resilient infrastructure requires national and sector-specific security goals that collectively represent the desired security posture. These goals should consider the physical, cyber, and human elements of CI/KR protection. Security goals will vary across and within sectors, depending on the internal structure and composition of a specific industry, resource, or other aspect of CI/KR.

Sample Sector-Specific Security Goal

The Telecommunications Sector will strive to ensure that the Nation's communications networks and systems are secure, resilient, and rapidly restored after a natural or man-made disaster.

Nationally, the overall goal of risk-reduction efforts is an enhanced state of CI/KR protection achieved through the implementation of focused risk-reduction and protective strategies within and across sectors. The risk management framework supports this goal by:

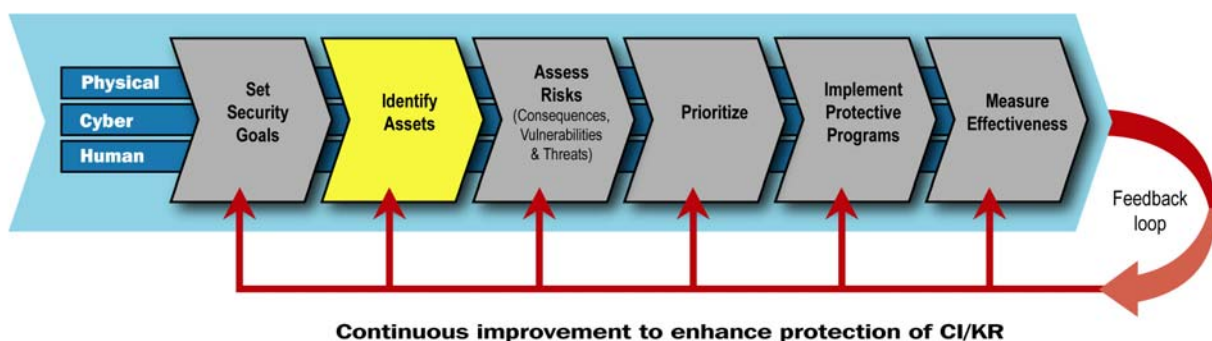
- Supporting the development of the national risk profile, a high-level snapshot summary of the aggregate risk and the protective status of all sectors. The national risk profile is developed by DHS in collaboration with other security partners, updated on an ongoing basis, and used to support strategic decision making and resource allocation;
- Enabling DHS, SSAs, and other security partners to determine the best course of action to reduce potential consequences or vulnerabilities. Some available options include encouraging voluntary implementation of focused risk-reduction and protective strategies (e.g., through public-private partnerships), pursuing incentive-related policies and programs, and undertaking regulatory action; and
- Using prioritized information to create, or identify, specific protective programs for CI/KR of the highest criticality based on risk. Depending on the protective program, resource allocation may occur at the Federal, State, local, or tribal level, or may be solely the responsibility of CI/KR owners and operators. International outreach and collaboration also may be required in many circumstances.

From a sector perspective, security goals:

- Define the protective (and, if appropriate, the response or recovery) posture that security partners seek to attain;
- Consider distinct assets, systems, networks, operational processes, business environments, and risk management approaches; and
- Vary according to the specific characteristics and security landscape of the affected sector, jurisdiction or locality.

Taken collectively, these goals guide all levels of government and the private sector in tailoring protective activities to address CI/KR protection needs.

3.2 Identify Assets



Once security goals are set, the next step is to identify assets. In order to do this, a comprehensive inventory of the Nation's infrastructure must be developed and maintained. CI/KR priorities may change quickly based on numerous factors, including the dynamic nature of the terrorist threat, evolving technologies, the economy, or damages resulting from a natural disaster. In order to appropriately manage risk in real time, the Federal government is required to maintain a comprehensive and up-to-date inventory that includes certain basic information on the assets, systems, and networks that comprise the Nation's

CI/KR. Additionally, this information must be compiled in a manner that allows it to be quickly scanned and analyzed to identify those assets, systems, or networks that may be the immediate focus of terrorist interest or may be directly in a storm's projected path. Once compiled, this inventory can be used to identify which assets, systems, or networks are nationally critical (i.e., become CI/KR) based on the most current national or sector risk profile. The inventory also can be used to inform national domestic incident management by helping to identify impacts on the Nation's CI/KR and establish priorities for restoration, remediation, and reconstruction following natural disasters or other catastrophic events.

The process for identifying national-level CI/KR involves a comprehensive approach that considers its physical, cyber, and human elements of an asset, system, or network. This approach includes gathering information on the relationships (e.g., dependencies and interdependencies) between various assets, systems, and networks to develop a more complete picture of the national CI/KR. It also includes working with international partners to obtain information on the foreign infrastructure and resources upon which U.S. CI/KR may rely.

A comprehensive national inventory, including the supporting information necessary to make decisions on asset, system, and network criticality, will be used to inform national CI/KR risk management efforts. Development and maintenance of this inventory require a collaborative effort among Federal, State, local, and tribal governments, and private sector security partners.

Elements of Infrastructure Assets, Systems, and Networks

An infrastructure **network** is a group of assets or systems that share information or interact with each other in order to provide infrastructure services to the Nation.

An infrastructure **system** is a collection of assets, resources, or elements that performs a process that provides infrastructure services to the Nation.

An infrastructure **asset** is something of importance or value to the process that provides infrastructure services. Assets are composed of one or more of the following elements:

Physical elements: Tangible property such as facilities, components, real estate, animals, and products.

Cyber elements: Electronic information and communications systems and the information contained in those systems (e.g., control systems), that are comprised of the hardware and software that processes, stores, and communicates information, or any combination thereof.

Human elements: Critical knowledge or expertise provided by people (e.g., tacit knowledge and job skills), which is susceptible to destruction, incapacitation, or exploitation through the individuals who possess or use such knowledge.

3.2.1 National Infrastructure Inventory

DHS, with support from all security partners, maintains and continuously improves a comprehensive inventory containing descriptive information on those assets, systems, and networks. This includes a cyber data framework to characterize each sector's unique cyber assets, systems, or networks. Currently, this inventory is maintained in the National Asset Database (NADB).

The NADB allows for the analysis that identifies which of these assets, systems, and networks are critical and therefore designated as CI/KR. SSAs and DHS work together and in concert with other security partners to ensure that the NADB data structure accurately represents each sector.

Information included in the NADB comes from a variety of sources:

- **Sector inventories:** SSAs provide and update inventories on a periodic basis to ensure that sector assets are adequately represented, and that sector and cross-sector dependencies and interdependencies can be identified and analyzed;
- **Voluntary submittals from security partners:** Owners and operators; State, local, and tribal governments; and Federal departments and agencies may submit information for DHS to consider for inclusion in the NADB at any time;
- **Results of studies:** Various government or commercially owned databases developed as the result of studies undertaken by trade associations, advocacy groups, and regulatory agencies may contain relevant information;
- **Periodic data calls:** DHS, in cooperation with SSAs and other security partners, may conduct data calls requesting the voluntary provision of specific information; and
- **Ongoing reviews of particular locations where threats are focused:** DHS- and SSA-initiated site assessments provide information on vulnerability; help to identify assets, systems, and networks and their dependencies and interdependencies; and quantify their value related to the potential consequences of an attack.

DHS, in coordination with SSAs, State and local governments, private sector owners and operators, and other security partners, gathers appropriate basic information for the full range of assets, systems, and networks. DHS also may coordinate with these security partners to gather additional information for assets, systems, and networks that, based on an initial screening, DHS determines to be of national significance. This additional information may include:

- System components that are central to the infrastructure mission and function;
- Dependencies and interdependencies (i.e., what the asset depends on in order to function, and which assets are reciprocally dependent upon it);
- Specific information on the asset, system, or network needed to conduct consequence analysis; and
- Assessment information that would enable DHS to conduct further comparative risk analysis in cooperation with the SSAs, the private sector, other security partners, or subject matter experts.

3.2.2 Protecting and Accessing Asset Information

The Federal government recognizes the sensitive, business, or proprietary nature of much of the information to be included in the NADB. DHS is responsible for protecting this information from unauthorized disclosure or use. Generally, submissions of asset information for inclusion in the NADB will be protected from unauthorized disclosure or use to the maximum extent allowed under applicable Federal, State, or local regulation, including Protected Critical Infrastructure Information (PCII) and security classification rules. Additionally, DHS will work to ensure that all data and licensing restrictions are enforced. DHS has implemented resilient and redundant security measures that apply to the NADB; these provide for system integrity and security, software security, and protection of the data therein.

Only select DHS employees have access to the NADB. Additional access may be provided using a tightly controlled, need-to-know system based upon relevant security classification guidelines. All users must apply for and be approved for access to the NADB based on appropriate authorization, clearance, and a need to know. Once this information is submitted, DHS verifies clearances and need to know, and assigns each individual role-based access authorization based on the scope of the information requested and required.

3.2.3 SSA Roles in Asset Identification

The processes that SSAs use to collect asset data and coordinate with DHS are described in the individual SSPs. The SSPs include descriptions of mechanisms for making data collection efforts more manageable, such as:

- Prioritizing the approach for outreach to different security partners;
- Identifying assets, systems, or networks of potential national-, regional-, or sector-level importance;
- Identifying, reviewing, and using existing databases; and
- Identifying specific assets, or classes of assets, for which additional data collection is unnecessary because of the inherently low risk associated with a potential terrorist attack.

SSAs help identify and obtain appropriate data for assets, systems, and networks that play a vital role in the Nation's security or economy – particularly those that involve significant dependencies or interdependencies. For example, a small manufacturer of pharmaceuticals or vaccines could be the sole U.S. manufacturer of that product. Similarly, a small plant could be the primary producer of a component vital to the defense industrial base. The identification of less visible assets makes the effort more time-consuming; however, it is a crucial part of the process if a true national risk profile is to be developed. More details on SSA roles and responsibilities, as well as those of other security partners, in creating the national catalog of CI/KR are contained in Appendix 4C.

3.2.4 Identifying Cyber Assets

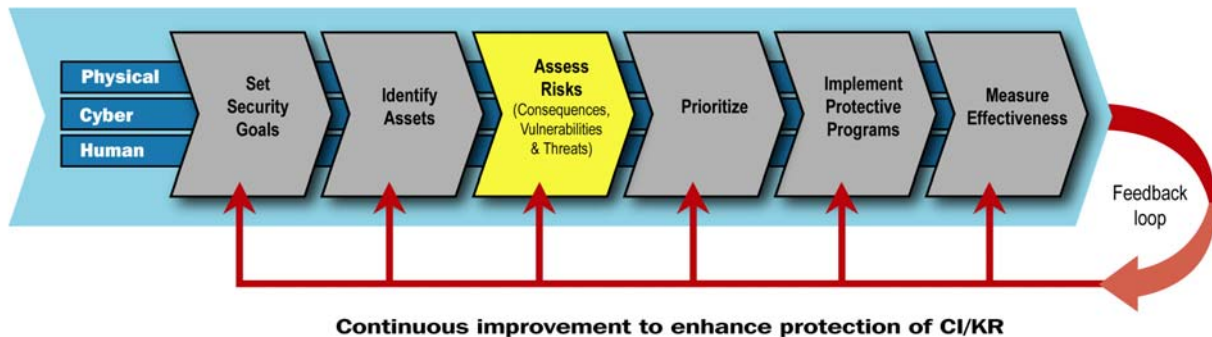
The NIPP addresses both physical and cyber CI/KR protection in an integrated manner.

Cyber assets represent a variety of hardware and software components; *cyber systems* are a set of cyber assets that interact to perform a particular function; and *cyber networks* are interconnected assets and systems that acquire or share information from each other. Cyber assets, systems, and networks should be identified individually or included as a cyber element of a physical asset, system, or network's description if they are associated with one. The following list provides examples of cyber assets, systems, or networks that exist in most, if not all, sectors:

- Digital control systems, including Supervisory Control and Data Acquisition (SCADA) systems and Process Control Systems;
- Automated access control systems supporting physical access control; and
- System interconnections (i.e., trusted connections), defined as the direct connection of two or more information technology systems owned by separate organizations.

DHS will support SSAs and other security partners by developing tools and methodologies to assist in identifying cyber assets, including those that involve multiple sectors. As needed, DHS will work with sector representatives to help identify cyber assets within the NIPP risk management framework.

3.3 Assess Risks



A variety of methodologies are available to facilitate comprehensive risk assessment. However, a common approach is needed to enable the setting of protection priorities across sectors. The first element of this approach is to establish a common definition and process for analysis of the basic factors of risk for CI/KR protection. In the context of homeland security, the three factors that combine to define *risk* are:

- **Consequence:** The range of loss or damage that can be expected from a successful attack;
- **Vulnerability:** The characteristic of, or flaw in, an asset, system, or network's design, location, security posture, or operation that renders it susceptible to destruction, incapacitation, or exploitation by terrorist or other intentional acts, mechanical failures, and natural hazards; and
- **Threat:** The likelihood that a particular target, or type of target, will suffer an attack or incident. In the context of risk from terrorist attack, threat likelihood is based on the analysis of the intent and the capability of an adversary.

To determine risk, consequences, vulnerabilities, and threats associated with the asset, system, or network are assessed and combined. Risk can be calculated for an asset, system, or network by sector, region, or nationally. The result is a comprehensive, systematic assessment of asset, system, sector, regional, or national risk that informs integrated risk-reduction activities.

DHS is working with SSAs, State and local governments, private industry, and other security partners to develop an approach that allows risk-based comparisons across sectors, while leveraging the assessments and analyses that have already been performed. This approach involves two parallel, mutually supportive efforts:

- Reconfiguring existing, widely used methodologies, or identifying simple means for normalizing the results of assessments performed using those methodologies, to support cross-sector comparability with minimal additional cost to security partners; and

- Collaboratively developing a risk-assessment process and methodology generally applicable across all sectors that asset owners and operators will be encouraged to use on a voluntary basis. Owners and operators who might find voluntary use advantageous are those who:
 - Have not previously performed a thorough risk assessment;
 - Need to update a previously completed assessment; and
 - Would like to use the primary DHS methodology for performing a new assessment.

To accomplish the first task above, the NIPP establishes a baseline criteria for risk assessment methodologies. The criteria provide a guide for improving existing methodologies or modifying them so the investment and expertise they represent can be used to support national-level, comparative risk assessment and resource prioritization.

To accomplish the second task, DHS is sponsoring the development of a suite of tools called Risk Analysis and Management for Critical Asset Protection (RAMCAP) that addresses the baseline criteria for risk assessment and can be used for national cross-sector risk assessment. This tool set will enable owners and operators to calculate potential consequences and vulnerability to an attack using a consistent system of measurements. It will also provide the means to convert and compare the results obtained from assessments performed with certain other approved methodologies.

The NIPP baseline criteria are set forth in the next section. The processes for assessing, analyzing, and combining the three specific components that make up risk – consequence, vulnerability, and threat – are explained in the following sections.

3.3.1 NIPP Baseline Criteria for Assessment Methodologies

Many owners and operators have performed vulnerability or risk assessments on the assets, systems, and networks under their control. To take advantage of this existing body of work, DHS plans to make every effort to use the results from previously performed assessments wherever possible. However, it should be noted that assessment work to date has varied widely both within and across sectors in its comprehensiveness, objectivity, inclusion of threat and consequence considerations, and physical/cyber dependencies.

3.3.1.1 Ensuring That Previous Assessments Can Be Used

To be acceptable for risk analysis, existing risk assessment tools and methodologies must be tested against the NIPP baseline criteria to ensure that they are suitable for use as part of a national-level risk analysis that relies on assessments that are comparable both within and across sectors. DHS and the SSAs will work with security partners to ensure that risk assessment tools and methodologies that meet the NIPP criteria will be available to security partners. DHS will leverage and incorporate work already done, to the greatest extent possible, and will help tailor existing tools to meet the baseline criteria as required.

3.3.1.2 Baseline Criteria

The NIPP baseline criteria for assessment methodologies consist of individual criterion that fall into two groups; these are listed specifically in Appendix 4A.

The first group tests the methodology to ensure that it will be *credible* to users of the analysis that the methodology produces. To be credible, a methodology must have a sound basis (it must have integrity), it must be complete, and it must be defensible. Tests for these criteria ask questions such as: Is the methodology based on classical risk analysis and security vulnerability analysis theory? Does it specifically address consequences, vulnerability, and threat?

The second group ensures that the methodology will support a comparative sector or national risk assessment. To be comparable, a methodology must be documented, transparent, reproducible, and accurate. Tests for these criteria ask questions such as: Does the methodology provide clear and sufficient documentation of the analysis process and the products that result from its use?

3.3.2 Consequence Analysis

The potential consequence of a terrorist attack or other hazard is the first factor to be considered in risk assessment. In the context of the NIPP, consequence is measured as the range of loss or damage that can be expected.

The consequences that are considered for the national-level comparative risk assessment are the consequences of national significance set forth in HSPD-7. These consequences can be divided into four main categories:

- **Health Impact:** Effect on human life and physical well-being (e.g., fatalities, injuries);
- **Economic Impact:** Direct and indirect effects on the economy (e.g., cost to rebuild asset, cost to respond to and recover from attack, downstream costs resulting from unavailability of product or service);
- **Psychological Impact:** Effect on the public's morale and confidence in national economic and political institutions; and
- **Governance Impact:** Effect on the government's ability to maintain order, deliver minimum essential public services, ensure the public's health and safety, and carry out national security-related missions.

A full consequence assessment takes into consideration health, economic, psychological and government impacts; however, accurately estimating potential indirect impacts can be difficult. When assessment of all categories of consequence is beyond the capabilities available for a risk analysis, the assessment should focus on health impact and direct economic impact.

3.3.2.1 Consequence Assessment Methodologies That Enable National Risk Analysis

DHS works with SSAs and other security partners to examine the inherent characteristics of assets, systems, or networks to identify the worst-reasonable-case consequences that are likely to result if the CI/KR in question is destroyed, incapacitated, or exploited. In order to support comparative risk analysis at the national level, security partners must use common terminology and metrics when assessing consequences and express the results in comparable units. To enable this, DHS works with security partners to develop consequence assessment methodologies that can be applied to a variety of asset, system, or network types and produce comparable quantitative consequence estimates. Specifically, DHS is working with industry partners to develop RAMCAP consequence assessment methodologies for various

1 CI/KR sectors and sub-sectors. When fully developed and implemented, the RAMCAP methodologies will
2 provide quantitative results that can be compared to the results of any other RAMCAP consequence
3 assessment, regardless of asset type.

4 Consequence analysis should address both the direct and indirect effects. Many assets depend on multiple
5 inputs to maintain functionality. For example, nearly all sectors rely on the Energy, Information Technology,
6 Telecommunications, Banking and Finance, and Transportation sectors. In some cases, a failure of an
7 asset in one sector will have a significant impact on the ability of an asset in the same or another sector to
8 perform necessary functions. As a result, consequence analysis must address both CI/KR dependency
9 (reliance on another asset or sector for functionality) and CI/KR interdependency (when two assets depend
10 on one another) for the purposes of NIPP risk assessment.

11 Various Federal and State entities, including national laboratories, are developing sophisticated models and
12 simulations to identify dependencies and interdependencies within and across sectors. The U.S.
13 government established the National Infrastructure Simulation and Analysis Center (NISAC) to support
14 these efforts. The NISAC charter is to develop advanced modeling, simulation, and analysis capabilities for
15 the Nation's CI/KR. These tools address physical and cyber cross-sector dependencies and
16 interdependencies related to all hazards, whether they are natural, accidental, or malevolent occurrences.
17 NISAC will enhance the Nation's understanding of infrastructure dependencies and interdependencies, and
18 better inform decision makers in the areas of policy analysis, investment, prevention and mitigation
19 planning, education, training, and crisis response.

20 The level of detail and specificity achieved by using sophisticated models and simulations may not be
21 practical or necessary for some assets, systems, or networks. In these circumstances, a simplified
22 dependency and interdependency analysis based on expert judgment can be used to provide the insight
23 necessary to make informed risk management decisions in a timely manner.

24 **3.3.2.2 Consequence Screening**

25 At present, many risk assessment methodologies use a consequence screening, or top-screen, to help
26 asset owners and operators decide whether a full risk assessment is necessary. DHS uses sector-specific
27 top-screens as part of the RAMCAP process. This approach allows facilities to identify their projected level
28 of consequence based on the nature of their business, proximity to significant population groups or other
29 CI/KR, relative importance to the national economy or military capability, and other similar factors. The
30 screening uses a standard form containing a few simple questions. If this initial screening determines that
31 an attack on an asset, system, or network is likely to result in consequences that are considered low from a
32 national perspective, owners and operators will not be asked by DHS or SSAs to perform additional
33 assessments. However, assets, systems, or networks that are screened out because of their relatively low
34 national risk may be considered critical on a State, regional, or local basis (e.g., a chemical facility that is
35 the primary employer in a given community). Accordingly, additional analysis may be warranted. Owners
36 and operators of infrastructures that are screened out using RAMCAP or another compatible assessment
37 methodology should consider whether their infrastructures require more detailed assessments in
38 conjunction with other State, regional, or local CI/KR protection efforts.

3.3.3 Vulnerability Assessment

Vulnerabilities are the characteristics of an asset, system, or network's design, location, security posture, or operation that render it susceptible to destruction, incapacitation, or exploitation by terrorist attacks or other malicious acts, mechanical failures, and natural hazards. They identify areas of weakness that could result in consequences of concern, taking into account intrinsic structural weaknesses, protective measures, resiliency, and redundancies.

Vulnerability assessments typically consist of the following key steps:

- Determine an appropriate vulnerability assessment strategy (e.g., self-assessment, State- or federally led assessment, expert reviews, or independent third-party assessment);
- Identify a methodology/tool appropriate for the particular type of asset at hand;
- Identify and group vulnerabilities using common threat scenarios;
- Identify dependencies and interdependencies with other assets and sectors;
- Consider vulnerabilities associated with physical, cyber, and human elements;
- Analyze benefits of existing protective programs; and
- Assess residual gaps to determine unresolved vulnerabilities.

3.3.3.1 Vulnerability Assessment Methodologies That Enable National Risk Analysis

Many different vulnerability assessment methodologies are used by security partners in the CI/KR sectors. The primary vulnerability assessment methodologies used in each sector are described in the respective SSPs. The SSPs also provide specific detail regarding how the assessments should be carried out (e.g., by whom, how often).

The results of vulnerability assessments must be comparable in order to be used in national-level, cross-sector analysis. DHS, in conjunction with various security partners, continuously improves RAMCAP vulnerability methodologies, which provides two means for producing comparable vulnerability assessment results. First, as part of the RAMCAP process, DHS develops sector-specific Security Vulnerability Assessment (SVA) modules for many sectors and sub-sectors. These RAMCAP SVA modules use a common approach that produces results that may be compared with other RAMCAP SVA module assessment results. Second, as part of the development of each RAMCAP SVA module, DHS and its security partners review vulnerability assessment methodologies that are used in the specific sector or sub-sector, and assess their compatibility with the DHS baseline criteria. If methodologies conform to the baseline criteria, then DHS can use assessment results produced using that methodology for the national comparative risk analysis. If the methodologies differ, DHS will work with security partners to either identify ways to adjust the methodology to conform to NIPP baseline criteria, or will develop "translators" to convert results developed with those methodologies into results that are comparable with the RAMCAP SVA modules. The specific approach will depend on the degree of difference and the robustness of the method in question.

3.3.3.2 SSA and DHS Analysis Responsibilities

SSAs are responsible for taking stock of, and facilitating, vulnerability assessment activities within their sectors; asset owners or operators typically perform these assessments. SSAs are also responsible for gathering, where possible, vulnerability assessment results for use in sector and national risk management efforts. Vulnerability assessment information may be submitted under the PCII Program (see Section 5.3, Protection of Sensitive Critical Infrastructure Information). SSAs are responsible for working with DHS to validate the results of those assessments for assets that are of the greatest concern from the sector perspective. For this validation review, SSAs should involve owners and operators in the review whenever practical.

DHS is responsible for ensuring that comprehensive vulnerability assessments are performed for CI/KR of national significance. This may involve DHS experts performing the vulnerability assessment in conjunction with the CI/KR owner or operator, or working with the CI/KR owner or operator or a third-party auditor to perform or to verify previously performed assessments.

DHS also conducts or supports vulnerability assessments that address specific needs of the NIPP's comprehensive approach to CI/KR protection. Such assessments:

- More fully investigate dependencies and interdependencies within and between sectors;
- Serve as a basis for developing common vulnerability reports that can help identify strategic needs for protective programs or R&D across sectors or sub-sectors;
- Fill selected gaps when sectors or asset owners or operators have not yet completed assessments and such studies are needed immediately; and
- Test and validate new methodologies or streamlined approaches for assessing vulnerability.

In some sectors and sub-sectors, vulnerability assessments have never been performed or may have been performed for only a small number of high-profile or high-value assets, systems, or networks. To help assist in closing this gap, DHS will work with SSAs to determine the common criteria for vulnerability assessments, particularly for nationally critical assets, systems, and networks and will provide:

- Vulnerability assessment tools to be used as part of self-assessment processes;
- Informative reports for industrial sectors, classes of activities, and high-consequence or at-risk special event sites;
- Generally accepted risk assessment principles for major classes of activities and high-consequence or at-risk special event sites;
- Assistance in the development and sharing of industry-based standards and tools;
- Suggest the frequency of assessments, particularly in light of emergent threats;
- Conduct site assistance visits and perform vulnerability assessments of specific CI/KR of particular concern as requested by owners and operators; and
- Disseminate cross-sector cyber vulnerability assessment best practices.

3.3.4 Threat Analysis

The remaining factor to be considered in the NIPP risk assessment process is the analysis of threat. In risk assessment, threat is the likelihood of a terrorist attack on a particular asset, system, or network. The estimate of this likelihood is typically based on an analysis of intent, means, and demonstrated capacity. Assessment of the current terrorist threat to the United States is derived from extensive study and understanding of terrorists and terrorist organizations, and frequently is dependent on analysis of classified information. DHS will provide U.S. government-coordinated assessments of potential terrorist threats derived from analysis of adversary intent and capability. These threat assessments will include postulated terrorist attack methods and will discuss what is known about terrorist interest in particular CI/KR sectors. Since international terrorists, in particular, have continually demonstrated flexibility and unpredictability, DHS will also frame known terrorist goals and collective capabilities to provide CI/KR owners and operators with a broad view of the potential threat.

In addition to physical attacks, terrorists may use the cyber domain as a platform to attack America's infrastructure. The use of innovative technology and interconnected networks in CI/KR operations improves productivity and efficiency, but also may increase the Nation's risk of cyber threats. Because of the interconnected nature of the cyber elements of CI/KR, cyber attacks can spread quickly and could have a substantial impact on the Nation's essential services and functions.

There are indicators that potential adversaries intend to conduct cyber attacks and are actively acquiring cyber attack capabilities. However, credible information on specific adversaries or attack modalities frequently is not available. Additionally, the increasing ease with which powerful cyber attack tools can be obtained and used places the ability to conduct cyber attacks within reach of groups or individuals wishing to do harm to the United States. Cyber-infrastructure threats are addressed in documents such as the *National Strategy to Secure Cyberspace*. A (classified) *National Intelligence Estimate of Cyber Threats to the U.S. Information Infrastructure* was published in 2004 and will be updated in 2006.

Another important consideration is the long-standing threat posed by insiders, or persons who have access to sensitive information and facilities based on job assignments. Insider threats can result from *intentional actions*, such as infiltration of the organization by terrorists, or *unintentional actions*, such as employees who are unknowingly manipulated into providing access to, or information about, CI/KR. Insiders can intentionally compromise the security of CI/KR through espionage or other harmful acts motivated by the rewards offered to them by a terrorist or other party. Employees who have no intention of endangering CI/KR or fellow employees can unintentionally compromise security if they are vulnerable to influence from outside threats through manipulation, blackmail, or other pressures. Others may become unwitting participants in the insider threat through lack of awareness of the need or methods to protect assets or employees (e.g., by leaving security badges and uniforms in open areas). CI/KR owners and operators and authorities with protection responsibilities frequently conduct screening and, if necessary, monitor employees in sensitive positions. These programs often have the support of Federal information or programs such as security clearances or job screening programs (e.g., hazardous material driver screening conducted by the Transportation Security Administration).

Threat Analysis Tools and Information

Threat analysis for CI/KR is undertaken by the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) within DHS in partnership with the U.S. government intelligence community, other Federal departments and agencies, and other supporting organizations. As called for in Section 201 of the Homeland Security Act of 2002, HITRAC is the organization that brings together intelligence and infrastructure specialists to ensure a complete and sophisticated understanding of the risks to U.S. CI/KR. HITRAC develops robust analytical products by combining intelligence, which includes all-source information, threat assessments, and trend analysis, with expert operational and practical knowledge, including an understanding of U.S. CI/KR vulnerabilities, potential consequences of attacks, and the effects of protective actions. This combination of intelligence and practical knowledge allows HITRAC to provide products for CI/KR risk assessment with actionable conclusions regarding terrorist threats and risks. Combining these two areas of expertise also allows HITRAC to identify and refine intelligence collection requirements so that the intelligence community can better support the national CI/KR protection mission.

HITRAC support for the NIPP includes information on the specific threats that are posed to U.S. CI/KR, as well as the information and planning tools that address the general threat environment that CI/KR protection planning must consider. Each is discussed below:

- **Specific Threat Information:** HITRAC monitors real-time intelligence streams to provide a fusion of intelligence analysis and infrastructure operational knowledge based on changing threat information. This analysis clarifies the implications of intelligence findings such as new information on targeted locations, sectors, or assets; new attack methods; or the potential timing of an attack. The analysis also informs any increase that may be needed in steady-state protective actions to respond to new threat information. In real time, specific threat information serves as a primary source for determining the probability of an attack on a given infrastructure asset, system, network, sector, or region. Over the longer term, specific threat information will also inform analysis of the general threat environment and the periodic updating of HITRAC products that are based on the general threat.
- **General Threat Environment Tools and Information:** HITRAC analyzes information about terrorist goals, objectives, and attack capabilities to assess how these would best suit particular terrorist attack profiles within each CI/KR sector. Unless specific intelligence and warnings about the selection of particular targets become available, this approach provides the best-informed picture of the threat. It provides analysts, decision makers, and CI/KR owners and operators with a broad, analytically based assessment of the threat facing each sector for use in risk assessment.

HITRAC integrates and analyzes law enforcement, intelligence, and other information that DHS collects from security partners to produce a number of threat products to support the NIPP. These analyses directly support national-level, cross-sector risk assessment, implementation, and associated sector risk assessments. They can be used to inform government and private sector protective action planning and resource investments. They also provide the analytic basis for situation reports on the current terrorist threat to U.S. CI/KR that are produced by DHS and other Federal partners on an as-needed basis.

Specialized products based on these analyses that directly support the NIPP and SSPs include a terrorist target selection matrix that outlines plausible means of attack for CI/KR sectors, a catalog of attack-specific

scenarios that details the actions required for an attack on a site or facility, and a sector-specific threat handbook that provides detailed information on the threat facing each sector:⁷

- **Terrorist Target Selection Matrix:** Because of the uncertainty of the current threat environment, security partners must employ a risk management approach that addresses the range of possible or probable threats. DHS provides threat assessments to SSAs and/or CI/KR owners and operators that are designed to support risk analysis for this range of threats. HITRAC developed the Terrorist Target Selection Matrix as an analytical tool for identifying which sectors are prone to various terrorist attack modalities; the Matrix is based on intelligence analysis of the major terrorist motives for attacks on the United States.

The Matrix provides a tool to help assess which attack methods are likely to be used against each of the CI/KR sectors and their primary sub-sectors by specifying the terrorist objectives that would be attained through each sector-attack combination. If intelligence analysis determines that terrorists are unlikely to use particular attack methods against a specific CI/KR sector or sub-sector, it is noted as a low-risk possibility and further consequence or vulnerability assessment may not be warranted. If a combination is determined to meet only one or two of the primary terrorist attack objectives, the sector is rated as modestly attractive to terrorists as a target. If terrorists can achieve all of their primary objectives by using a particular attack method against a particular sector or sub-sector, the situation warrants careful attention and priority for consequence and vulnerability analysis. Depending on the results of the consequence and vulnerability assessment, the attack/sector combination may pose a likely target and a candidate for protective measures to offset the risk. When combined with consequence analysis, the screening that this form of threat analysis provides focuses subsequent risk assessments on those attack/sector combinations that may offer a high return for protective program investments or a substantial benefit for protective actions.

The Terrorist Target Selection Matrix supports national-level risk assessments, sector-specific application of the NIPP risk management framework, and development and implementation of the SSPs.

- **Attack-Specific Threat Scenarios:** Threat scenarios provide a common, detailed description of potential attack methods. They provide detailed vignettes of the specific attack methods, techniques, and actions terrorists are likely to use against specific types of U.S. CI/KR. The scenarios are based on known terrorist capabilities or on their stated intent as derived from intelligence and the study of terrorist tactics, techniques, and capabilities.

Threat scenarios are specific enough to be used by facility security officers for operational planning of protective actions. This use allows security forces to identify elements of attack scenarios that can be observed and reported, and elements that cannot be observed, but that could constitute the basis for valid information requests.

This product supports facility-level threat surveillance by security forces, owner and operator requests for intelligence information, and protective action planning. It also provides detailed threat information for the sector-specific threat handbook described below.

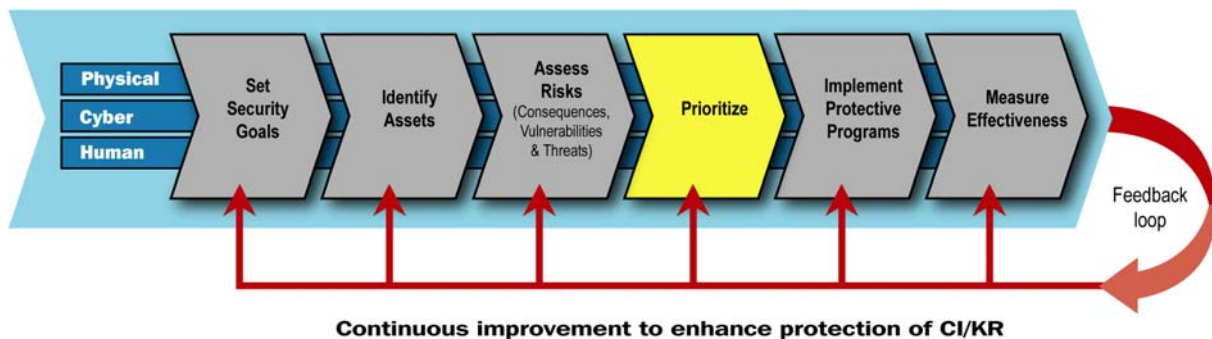
⁷ It should be noted that *threat*, as used here, is the estimated probability value assigned for a specific asset, system, network, sector, or region for the purposes of calculating that item's level of risk. This differs from *threat scenarios*, which are generalized descriptions of potential methods of attack that are used to inform consequence and vulnerability assessments.

- **Sector-Specific Threat Handbook:** HITRAC uses the information developed through the matrix and the threat scenarios to produce Sector-Specific Threat Handbooks that provide compilations of the potential terrorist threats posed to each of the CI/KR sectors. HITRAC works with the private sector to develop and provide these sector- and sub-sector-specific threat products and addresses private sector information needs. These handbooks include known specific and general terrorist threat information for each sector, as well as relevant background information such as terrorist objectives and motives as they apply to the sector. The handbooks will be updated on a routine basis, including the most current intelligence findings or operational trend analyses. Each sector-specific threat report will include the Terrorist Target Selection Matrix to provide overall CI/KR context for the sector and will specify those Attack-Specific Threat Scenarios that are relevant to the sector to provide the detail necessary for SSP development, implementation, and security-related planning.

This product supports sector-level planning, including SSP development. It also provides detailed threat information for facilities associated with the sector.

In addition to these specific products, HITRAC will produce special, longer term strategic assessment and trend analysis that helps define the evolving threat to the Nation's CI/KR. These products are designed to support the NIPP, inform SSP development, and contribute to operational and investment planning by the private sector and government for CI/KR protection.

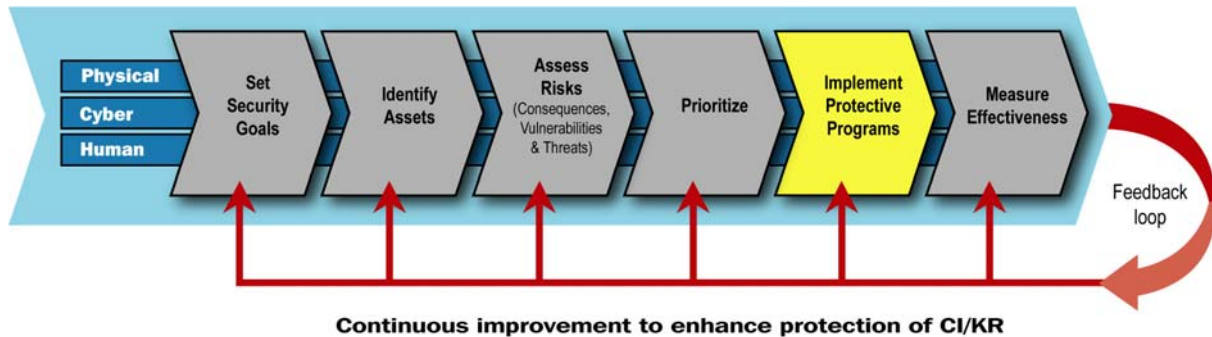
3.4 Prioritize



After risk-related data have been collected, combined, and analyzed, the results of the risk assessments are prioritized to help identify where risk reduction is most pressing, and to subsequently determine what protective actions should be taken. Prioritization requires a comparison of the relative levels of asset and sector risk along with options for achieving the established security goals.

Differences in assessment methodologies and characterizations of risk often result in significant differences in the consistency and comparability of corresponding risk measures. Whenever possible, DHS uses analysis-based normalization tools to convert risk assessment results from analyses that do not meet the NIPP baseline criteria into measures that can be used by DHS for national-level comparison. The RAMCAP process produces results that can be used directly for the national risk assessments without a separate normalization step. Where normalization is not possible, DHS will encourage the use of either the RAMCAP methodologies or other analytical tools that meet the NIPP baseline criteria.

3.5 Implement Protective Programs



The Nation's CI/KR is widely distributed in both a physical and logical sense. Effective CI/KR protection requires both distributed implementation of protective programs by security partners, and centralized national leadership to ensure implementation of a comprehensive, coordinated, and cost-effective approach that helps to reduce the risks to the Nation's most essential assets, systems, and networks. At the implementation level, protective programs consist of actions undertaken by various security partners. From the leadership perspective, programs are structured to address coordination and cost effectiveness. These two aspects of protective program implementation are discussed in the following sections.

3.5.1 Protective Actions

Protective actions may involve measures designed to prevent, deter, and mitigate terrorist attacks on CI/KR assets; reduce vulnerability to an attack; and enable timely, efficient response and restoration in a post-event situation, whether a terrorist attack or natural disaster. Protective actions attempt to indirectly affect the threat and directly affect vulnerability and consequence as follows:

- **Deter:** Cause the potential attacker to perceive that the risk of failure is greater than that which they find acceptable. Examples include improved awareness and security (e.g., restricted access, vehicle checkpoints) and enhanced police and/or security officer presence;
- **Devalue:** Reduce the attacker's incentive by reducing the target's value. Examples include developing redundancies and backup systems or individuals, or deemphasizing the importance of particular special events;
- **Detect:** Identify potential attacks and validate and/or communicate the information, as appropriate. General detection activities include intelligence gathering, analysis of surveillance activities, and trend analysis of law enforcement reporting. For specific assets, examples include intrusion-detection systems, network monitoring systems, operation alarms, surveillance, detection and reporting, and employee security awareness programs; and
- **Defend:** Protect assets by preventing or delaying the actual attack, or reducing an attack's effect on an asset. Examples include perimeter hardening by enhancing buffer zones, fencing, structural integrity, and cyber defense tools such as antivirus software.

Protective programs also may include actions that have an impact on the consequences should an attack occur. These actions are focused on the following aspects of preparedness:

- **Mitigate:** Lessen the potential impacts of an attack, such as introducing system redundancy and resiliency, reducing asset dependency, or isolating downstream assets;
- **Respond:** Design to enable rapid reaction and emergency response to an attack, such as conducting exercises and having adequate crisis response plans, training, and equipment; and
- **Recover:** Allow the sector to resume operations quickly and efficiently, such as developing the continuity-of-operations plans.

Generally, it is considered more cost-effective to build security into CI/KR than to retrofit CI/KR with security measures after initial construction. Accordingly, it is recommended that risk management, robustness, and appropriate security elements be incorporated into the design and construction of new CI/KR when it is built.

In situations where robustness and resiliency are keys to CI/KR protection, providing protection at the system level rather than at the asset level may be more effective and efficient (e.g., if there are many similar facilities, it may be easier to allow other facilities to provide the infrastructure service rather than to protect each facility).

3.5.2 Characteristics of Effective Protective Programs

Characteristics of effective CI/KR protective programs include, but are not limited to, the following:

- **Comprehensive:** Effective protective programs must address the physical, cyber, and human elements of CI/KR, as appropriate, and consider long-term, short-term, and sustainable activities. SSPs describe programs and initiatives to protect assets within the sector (e.g., operational changes, physical protection, equipment hardening, system resiliency, backup communications, response plans, and security system upgrades);
- **Coordinated:** Because of the highly distributed and complex nature of CI/KR sectors, the responsibility for protecting assets must be coordinated:
 - CI/KR owners and operators (public or private sector) are responsible for protecting property, information, and people, through measures that manage business risk to help ensure more resilient operations and more effective loss prevention. These measures include increased awareness of terrorist threats and implementation of operational responses to reduce vulnerability (e.g., changing daily routines and keeping computer software and virus checking applications up to date);
 - State, local, and tribal authorities are responsible for providing or augmenting protective actions for assets, systems, and networks that are critical to the public within their jurisdiction and authority. They develop protective programs, supplement Federal guidance and expertise, implement certain relevant Federal programs (i.e., the Urban Area Security Initiative or the Buffer Zone Protection Program), and provide specific law enforcement personnel as needed. When appropriate, they have access to Federal resources to meet State, local, or tribal CI/KR protection priorities;

- Federal agencies are responsible for enabling protection for CI/KR that is critical from a national perspective and coordinating the efforts of security partners and the use of resources from different funding sources. DHS, SSAs, and other Federal departments and agencies carry out these responsibilities while respecting the authorities of State, local, and tribal governments, and the prerogatives of the private sector;
- SSAs, in conjunction with security partners, provide information on the most effective long-term protective strategies and enable the development and implementation of protective programs for their sectors. For some sectors, this includes the development and sharing of best practices and criteria, guidance documents, and tools;
- DHS, in collaboration with SSAs and other public and private sector partners, serves as the national focal point for the development, implementation, and coordination of protective programs (including cybersecurity efforts) for those assets that are critical from a national perspective.
- **Cost-Effective:** Effective protective programs seek to use resources efficiently by focusing on protective actions that offer the greatest reduction in risk for any given expenditure. The following is a discussion of factors that should be considered when assessing the cost-effectiveness and public benefits derived through implementation of CI/KR protection initiatives:
 - **Operating with full information and lowering coordination costs:** The NIPP provides mechanisms to enable the use of information regarding threats and corresponding protective actions.

This begins with the risk assessment process itself, which allows security partners to make their investments where they will have the greatest benefit. It includes information sharing among security partners, provision of a dedicated communications network, and the use of established, interoperable industry and trade association communications mechanisms. The NIPP also lowers the cost of coordination through such mechanisms as security partnership arrangements and, where appropriate, the use of a regulatory framework to encourage or drive action.
 - **Addressing the present-future tradeoff in long lead time investments:** The NIPP provides the processes and coordinating structures that allow State, local, and tribal governments and private sector partners to effectively use long lead time approaches to CI/KR protection.
 - **Providing for appropriate burden sharing among security partners:** With appropriate burden sharing for CI/KR protection, CI/KR owners and operators are responsible for protecting property, information, and people through measures that manage business risk to help ensure more resilient operations and more effective loss prevention. State, local, and tribal authorities are responsible for providing or augmenting protective actions for assets, systems, and networks that are critical to the public within their jurisdiction and authority. Federal agencies are responsible for enabling protection for CI/KR that is critical from a national perspective. When appropriate, they make Federal resources available for selected State, local, or tribal CI/KR protection priorities.
 - **Matching the underlying economic incentives of each security partner to the extent possible:** The NIPP supports mechanisms that rely on market-based economic incentives wherever possible by relying on security partners to undertake those efforts that are in their own interest and complementing those efforts with additional resources where necessary. This builds on efforts that have proven to be effective and are consistent with best business practices, such as

1 allowing owners and operators to select the measures best suited to their particular risk situation
2 and needs.

- 3 ➤ **Addressing the “externalities” associated with providing benefits to the public at large:**
4 Protective actions for CI/KR that provide benefits to the public at large go beyond the actions that
5 benefit owners and operators, or even those that benefit the public who resides in a particular
6 State, region, or locality. Such additional actions reflect different levels of the public interest – some
7 CI/KR is critical to the national economy and to national well-being; some CI/KR is critical to a
8 State, region, or locality; some CI/KR is critical only to the individual CI/KR owner and operator.
9 Actions to protect the public’s interest that require investment beyond the level that those directly
10 responsible for protection are willing and able to provide, must be of sufficient priority to warrant the
11 use of the limited resources that can be provided from public funding or may require appropriate
12 incentives to encourage the private sector to undertake them.

- 13 • **Risk-Based:** Protective programs focus on reducing risk by affecting the elements of risk, individually
14 or collectively. Protective actions should be designed to allow measurement, evaluation, and feedback
15 based on risk reduction. This allows asset owners and operators and SSAs to reevaluate risk after the
16 program has been implemented, as well as to measure its effect on sector security. Protective
17 programs use different mechanisms for addressing each element of risk and combine their effects to
18 achieve overall risk reduction. These mechanisms include:

- 19 ➤ **Consequences:** Protective programs that directly limit or manage consequences by reducing the
20 possible damage resulting from a successful attack or a natural hazard as redundant system
21 design, backup systems, and alternative sources for raw materials or information are examples of
22 these mechanisms.

- 23 ➤ **Vulnerability:** Protective programs directly reduce vulnerability by decreasing the susceptibility to
24 destruction, incapacitation, or exploitation by correcting flaws or weaknesses in asset, system, and
25 network design.

- 26 ➤ **Threat:** Protective programs indirectly reduce threat by making assets, systems, or networks less
27 attractive targets to terrorists by lessening vulnerability and lowering consequences. This means
28 that terrorists are less likely to achieve their objectives and therefore less likely to pose a threat to
29 the CI/KR in question.

30 3.5.3 Protective Programs, Initiatives, and Reports

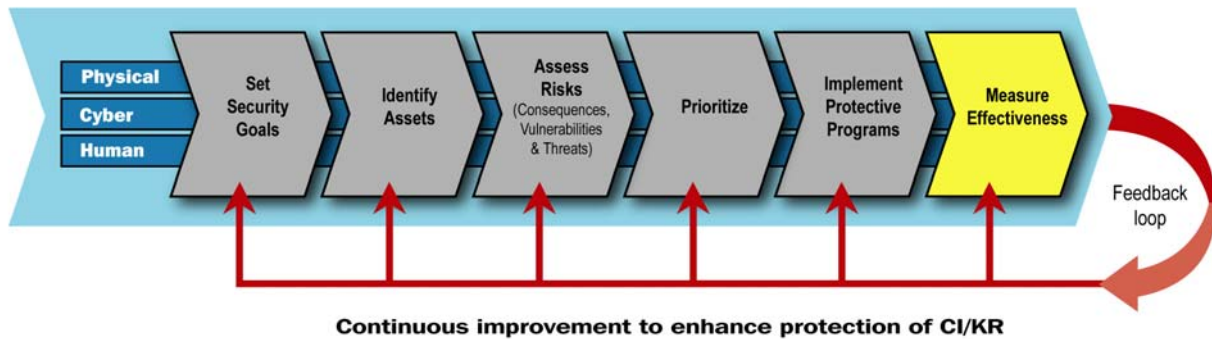
31 DHS, in collaboration with other security partners, undertakes a number of protective programs, initiatives,
32 activities, and reports that support CI/KR protection. Many of these are available or provide resources to
33 security partners. These activities span a wide range of efforts, including:

- 34 • **Buffer Zone Protection Program (BZPP):** Grant program designed to provide resources to State, and
35 local law enforcement to enhance security “outside the fence.”
- 36 • **Site Assistance Visits (SAVs):** Facility security assessments designed to facilitate vulnerability
37 identification and mitigation discussions between the Federal government and individual owners and
38 operators.
- 39 • **Government Forum of Incident Response and Security Teams:** Facilitates interagency information
40 sharing for cyber system protection.

The activities also include developing and providing informational reports, such as the Characteristics of Common Vulnerabilities reports and the Indicators of Terrorist Activity reports, which are distributed to all State and Territorial homeland security offices.

A detailed discussion of DHS-supported programs, initiatives, activities, and reports is provided in Appendix 4B.

3.6 Measure Effectiveness



Measuring effectiveness drives continuous improvement of CI/KR protective actions and programs at the sector level and overall program performance at the national level. The NIPP uses a metrics-based system to provide feedback on efforts to attain the goals and objectives articulated in Chapter 1. The metrics also provide a basis for establishing accountability, documenting actual performance, facilitating diagnoses, promoting effective management, and reassessing goals and objectives. Metrics offer a quantitative assessment to affirm that specific objectives are being met or to articulate gaps in the national effort. They enable identification of corrective actions and provide decision makers with a feedback mechanism to help them make appropriate adjustments. Lessons learned from exercises and actual incidents and alerts provide additional objective input into the process.

3.6.1 NIPP Metrics and Measures

The NIPP risk management framework uses three types of quantitative indicators to measure program effectiveness:

- **Descriptive Metrics:** Used to understand sector resources and activities; they do not reflect CI/KR protection performance. Examples include the number of facilities in a jurisdiction; the population resident or working within typical incident effects footprints; and the number, nature, and location of suppliers in an infrastructure service provider's supply chain.
- **Process (or Output) Metrics:** Measure whether specific activities were performed as planned, tracking the progression of a task, or report on the output of a process such as inventorying assets. Process metrics show progress toward performing the activities necessary to achieve CI/KR protection goals. They also help build a comprehensive picture of CI/KR protection status and activities. Examples include: the number of protective programs implemented in a specific fiscal year and the level of investment for each; the number of detection systems installed at facilities in a given sector; the

1 proportion of a facility's work force that has completed training; and the level of response to a data call
2 for asset information.

- 3 • **Outcome Metrics:** Track progress toward a strategic goal by beneficial results rather than level of
4 activity, which indicates progress toward specific goals or objectives. As the NIPP is implemented,
5 process metrics will be deemphasized in favor of outcome metrics. Examples include the reduction of
6 risk measured by comparing one year's comparative analysis for a specific sector to another, and the
7 overall risk reduction achieved nationally by a particular CI/KR protection initiative.

8 Incorporating all three of these quantitative indicators, NIPP metrics are divided into two groups: (1) core
9 metrics, and (2) sector-specific metrics. Core metrics are basic measures that can be tracked across each
10 sector to enable comparison and analysis between different types of CI/KR. Sector-specific metrics are
11 tailored to the unique characteristics of each sector and will be used to assist in monitoring progress in a
12 specific sector.

13 **3.6.1.1 Core Metrics**

14 Core metrics being developed are common across all sectors and are a set of descriptive, process, and
15 outcome data that enable measurement of progress in SSP implementation. Examples are total number of
16 assets by class, number of assets with potential for medium or high consequence, assets with completed
17 vulnerability analyses, etc.

18 These core metrics will be consistent with the National Preparedness Goal and its supporting Universal
19 Task List and Target Capabilities List. Resources will be allocated to those activities that best accomplish
20 CI/KR protection goals; activities that do not advance these goals will be redesigned or eliminated over
21 time.

22 **3.6.1.2 Sector-Specific Metrics**

23 DHS works with SSAs and other security partners, as appropriate, to develop and implement sector-
24 specific metrics. For example, sector-specific metrics might include the percentage of shipments moving
25 through a specific port that are subjected to detailed screening, or the change in time required to obtain
26 results from test samples.

27 **3.6.2 Gathering Performance Information**

28 DHS works with SSAs and other security partners to gather the information necessary to measure the level
29 of performance associated with each set of core and sector-specific metrics. Given the inherent differences
30 in CI/KR sectors, a "one size fits all" approach to gathering this information is not appropriate. DHS will
31 work with each SSA, in conjunction with security partners, to determine the appropriate method that will be
32 included in their SSP. SSAs will identify and, as appropriate, share or facilitate the sharing of best practices
33 based on the effective use of metrics to improve program performance.

3.6.3 Assessing Performance and Reporting on Progress

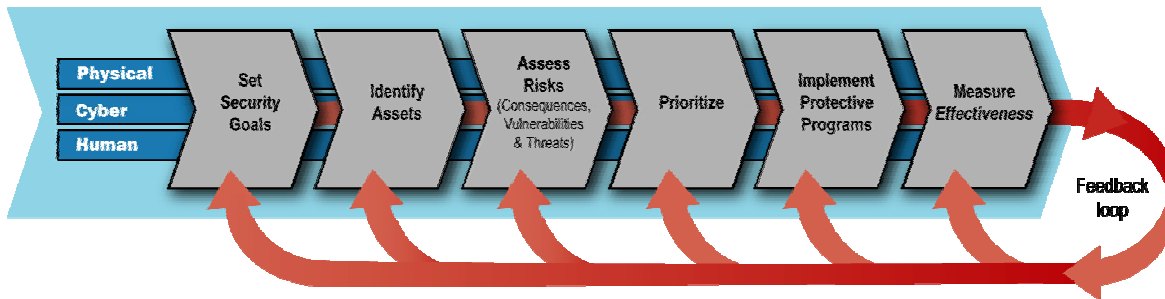
HSPD-7 requires SSAs to provide the Secretary of Homeland Security with Annual Reports that serve as a primary tool for assessing performance and reporting on progress. The Annual Reports are developed by each SSA to:

- Provide a common vehicle across all CI/KR sectors for communicating CI/KR protection performance and progress to security partners and other government entities;
- Establish a baseline of existing sector-specific CI/KR protection programs and initiatives;
- Identify SSA resource requirements and planned departmental CI/KR budget recommendations;
- Determine and explain how sector efforts support the national effort;
- Provide an overall progress report for the CI/KR sector and measure that progress against the national CI/KR protection goals for that sector;
- Provide feedback to DHS, the CI/KR sectors, and other government entities that will be used as the basis for the continuous improvement of the CI/KR protection program; and
- Help to identify best practices from successful programs and share these within and among sectors.

DHS works with SSAs to assess progress made toward goals in each sector based on these reports. DHS then compiles them into a national cross-sector report that describes overall progress toward CI/KR protection goals across the Nation. The initial sector program assessment is used to establish a baseline against which improvement will be measured. The cross-sector report includes the near-term requirements needed to make deliberate progress toward long-term goals. A more detailed discussion of the resource allocation process for CI/KR protection is included in Chapter 7.

In addition to these annual reports, SSAs regularly update their measurements of CI/KR status and protection levels to support DHS status reports. By maintaining a regularly updated knowledge base, DHS is able to quickly compile real-time CI/KR status and protection posture reports to respond to changing circumstances as indicated by tactical intelligence assessments of terrorist threats or natural disaster damage reports. This helps inform resource allocation decisions during incident response and other critical operations supporting the homeland security mission.

3.7 Using Metrics and Performance Measurement for Continuous Improvement



Continuous Improvement to enhance protection of CI/KR

By using NIPP metrics to compare performance to goals, security partners adjust and adapt the Nation's CI/KR protection approach to account for progress achieved, as well as for changes in the threat and other relevant environments. At the national level, NIPP metrics will be used to focus Federal and security partner attention on areas of CI/KR protection that warrant additional resources or other changes. If a comparison of performance and goals using NIPP metrics reveals that there is insufficient progress toward goals (e.g., information-sharing mechanisms have not been established and risk assessments have not been conducted, or one or more sectors have a significant portion of their assets rated as high risk), DHS and its security partners will make policy decisions and undertake actions to focus CI/KR protection efforts on addressing those particular areas of concern.

In addition, the information gathered as part of the risk management framework process will drive specific CI/KR protection activities. For instance, every time a protective program is implemented, there is a change in the consequences and vulnerabilities associated with the assets affected by the program. Accordingly, the national risk profile is reviewed routinely to ensure that current and prospective allocations of resources are appropriate in light of recently implemented protective actions or other factors, such as increased understanding of potential system-wide cascading consequences, new threat intelligence, etc.

In addition to quantitative measures, the NIPP provides mechanisms for qualitative feedback that can be applied to augment and improve the effectiveness and efficiency of public and private sector CI/KR protective programs. DHS works with security partners to identify and share lessons learned and best practices for all aspects of the risk management process. DHS also works with SSAs to collect relevant input from security partners and other sources that can be used as part of the national effort to continuously improve CI/KR protection.

4. Organizing and Partnering for CI/KR Protection

The enormity and complexity of the Nation's CI/KR, the distributed character of its associated protective architecture, and the uncertain nature of the terrorist threat make the effective implementation of protection efforts an enormous challenge. To be effective, the national CI/KR protection strategy must be based on a thorough understanding of these variables and implemented through a coordinated, unified, national approach.

4.1 Leadership and Coordination Mechanisms

The coordination mechanisms described below establish linkages among CI/KR protection efforts at the Federal, State, regional, local, tribal, and international levels, and between private sector and non-governmental security partners. The structures described below provide a national umbrella that fosters relationships and facilitates coordination within and across CI/KR sectors:

- **National-Level Coordination:** The DHS Office of Infrastructure Protection (DHS/OIP) facilitates overall development of the NIPP and SSPs, provides overarching guidance, and monitors the full range of associated coordination activities and performance metrics.
- **Sector Partnership Coordination:** The NIPP Federal Senior Leadership Council, Private Sector Cross-Sector Council, and individual Sector and Government Coordinating Councils create a structure through which representative groups from all levels of government and the private sector can collaborate and develop consensus approaches to CI/KR protection.
- **State, Territorial, Local, and Tribal Coordination:** Designated State Administrative Agencies, Homeland Security Advisors⁸, and emergency managers coordinate protection-related activities of State, local, and tribal government planners, administrators, and responders.
- **Regional Coordination:** Regional partnerships, groupings, and governance bodies enable CI/KR protection coordination among security partners within and across geographical areas and sectors. Such bodies are composed of representatives from industry and State, local, and tribal entities located in whole or in part within the planning area for a high threat target, urban area, or sector-based region. They are organized to address common approaches to natural or man-made hazards.
- **International Coordination:** The United States-Canada-Mexico Security and Prosperity Partnership; the North Atlantic Treaty Organization's (NATO's) Senior Civil Emergency Planning Committee; and certain government councils, such as the Committee on Foreign Investment in the United States, enable a range of CI/KR protection coordination activities associated with established international agreements.

4.1.1 National-Level Coordination

DHS oversees the coordination and integration of national-level CI/KR protection activities through the DHS/OIP. In support of security partner coordination, DHS:

⁸ The chief designated official responsible for homeland security efforts in a particular State or Territory.

- Leads, integrates, and coordinates the execution of the NIPP, in part by acting as a central clearinghouse for the information sharing and coordination activities of the individual sector governance structures;
- Facilitates the development and ongoing support of these security partner governance/coordination structures/models;
- Ensures that NIPP revisions undergo a comprehensive national review prior to issuance;
- Ensures that effective policies, approaches, guidelines, and methodologies regarding partner coordination are developed and disseminated to enable SSAs and other security partners to carry out NIPP responsibilities;
- Acts as a facilitator for the sharing of best practices and lessons learned; and
- Facilitates security partner participation in readiness exercises.

4.1.2 Sector Partnership Coordination

Protecting the Nation's CI/KR requires the development of partnerships between and among government and private sector infrastructure owners and operators at all levels, both within and across sectors. The goal of these partnerships is to establish the context, framework, and support for coordination and information-sharing activities required to implement and sustain a full spectrum of protective actions.

The NIPP relies on the sector partnership model, illustrated in Figure 4-1, as the primary means of coordinating CI/KR efforts. The sector partnership model encourages formation of Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs) as described below. DHS also provides guidance, tools, and support so that these groups can work together to carry out their respective roles and responsibilities. SCCs and corresponding GCCs work in tandem to create a coordinated national umbrella for CI/KR protection across sectors.

Cross-sector issues and interdependencies will be addressed between the SCCs through the Partnership for Critical Infrastructure Security (PCIS). The PCIS membership is comprised of one or more members and their alternates from each of the SCCs, as designated by each individual SCC. The corollary NIPP Federal Senior Leadership Council is comprised of one or more representatives and their alternates from each individual GCC. These cross-sector bodies will convene in joint session, as appropriate, to address cross-cutting CI/KR protection issues. The NIPP related functions of the cross-sector bodies include activities to:

- Provide coordination, communication, and information sharing across sectors and between and among DHS, the SSAs, supporting Federal departments and agencies, and other public and private sector security partners;
- Identify issues shared by multiple sectors that would benefit from common investigations and/or solutions;
- Identify and promote best practices from individual sectors that have applicability to other sectors;
- Contribute to cross-sector prioritization efforts, as appropriate; and
- Provide input to the government on R&D efforts that would benefit multiple sectors.

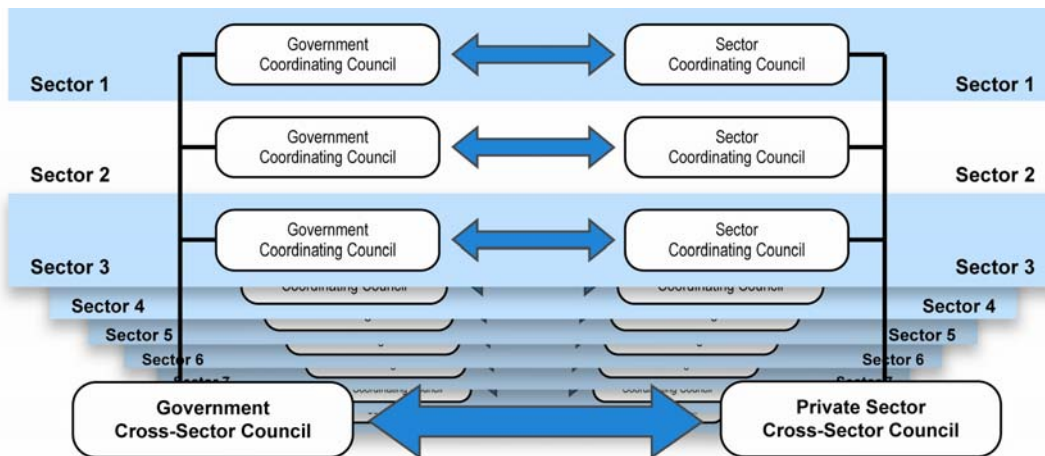


Figure 4-1: Sector Partnership Model

4.1.2.1 Sector Coordinating Councils

The sector partnership model encourages CI/KR owners and operators to create or identify an SCC as the principal entity for coordinating with the government on a wide range of CI/KR protection activities and issues. SCCs should be self-organized, self-run, and self-governed, with a spokesperson designated by the sector membership. Specific membership will vary sector to sector, reflecting the unique composition of each sector; however, they should be broadly representative of a broad base of owners, operators, associations, and other entities – both large and small – within a sector.

The SCCs provide the framework to enable owners and operators for internal coordination on a wide range of sector-specific CI/KR protection activities and issues. The primary functions of an SCC include:

- Represent a primary point of entry for government into the sector for addressing the entire range of infrastructure protection activities and issues for that sector;
- Serve as a strategic communication and coordination mechanism between owners, operators and suppliers, and with the government during response and recovery;
- Identify, implement, and support the information sharing capabilities and mechanisms that are most appropriate for the sector. Information Sharing and Analysis Centers (ISACs) may perform this role, if so designated by the SCC;
- Facilitate inclusive organization and coordination of the sector's policy development regarding CI/KR protection planning and preparedness; exercises and training; and associated plan implementation activities and requirements;
- Advise on integration of State, regional, and local planning initiatives with Federal initiatives, such as the State and local role in SSPs, the NIPP and the NRP; and
- Provide input to the government on R&D efforts and requirements.

4.1.2.2 Government Coordinating Councils

A GCC is formed as the government counterpart for each SCC to enable interagency and cross-jurisdictional coordination. The GCC is comprised of representatives across various levels of government (i.e., Federal, State, local, and tribal), as appropriate to the security landscape of each individual sector. At the national level the NIPP Federal Senior Leadership Council fulfills this role.

The GCC coordinates strategies, activities, policy, and strategic communications across government entities within each individual sector. The primary functions of a GCC include:

- Provide interagency strategic coordination and communication at the sector level through partnership with DHS, the SSA, and other supporting Federal departments and agencies;
- Participate in planning efforts relating to the development and implementation of the NIPP Base Plan and SSPs;
- Coordinate strategic communications, issue management, and resolution among government entities within the sector; and
- Coordinate with and support efforts of the SCC to plan, implement, and execute the Nation's CI/KR protection mission.

4.1.3 State, Local, and Tribal Government Coordination

State Homeland Security Advisors (HSAs) serve as points-of-contact for DHS, governments at all levels, and CI/KR owners and operators. HSAs serve as vital components of the sector partnership model, providing guidance on State-level CI/KR protection strategies and programs. Other State Administrative Agencies, SAAs, and entities, as designated by the Governor, support development of homeland security strategies, implement strategic goals and objectives, and administer Federal preparedness assistance. In some cases, State Administrative Agencies also perform the HSA function, while in other cases, these positions are staffed separately. States also use State agencies as sector leads, much as the Federal government has identified SSAs.

4.1.4 Regional Coordination

Regional partnerships, organizations, and governance bodies across the country enable CI/KR protection coordination among security partners within and across geographical areas to engage in planning and program implementation aimed at a common hazard or threat environment. These groupings include public-private partnerships that cross-jurisdictional, sector, and international boundaries and take into account dependencies and interdependencies. They are typically self-organizing and self-governing.

Regional organizations, whether inter- or intra-state, vary widely in terms of mission, composition, and functionality. Regardless of the variations, these organizations provide structures at the operational level that are helpful in addressing cross-sector CI/KR planning and protection program implementation within the given geographical areas. In many instances, State Homeland Security Advisors serve as focal points for regional initiatives and provide linkages between the regional groups and the sector partnership model. However, based on the nature or focus of the regional initiative, these groups also may link into the sector

partnership model, as appropriate, through SCCs or GCCs. Additionally, DHS selectively institutes cross-region councils based on the partnership model to address issues that involve several regions.

The Pacific NorthWest Economic Region provides an example of a regional organization structured as a public-private partnership that includes legislators, governments, and businesses in five States and three Canadian provinces. The Region, established by statute in all member States and Provinces, sponsored bi-national, multi-jurisdictional CI/KR protection interdependency exercise, and developed an action plan outlining several physical and cyber CI/KR protection projects.

4.1.5 International CI/KR Protection Cooperation

Most CI/KR assets, both physical and cyber, are interconnected with the global infrastructures that have evolved to support modern economies. Each of the CI/KR sectors is linked in varying degrees to global energy, transportation, telecommunications, cyber, and other infrastructures. This global system creates benefits and efficiencies, but also brings interdependencies and vulnerabilities. The Nation's prosperity and way of life depend on these "systems of systems," which must be protected both at home and abroad.

The NIPP strategy for international CI/KR protection coordination and cooperation is focused on:

- Instituting effective cooperation with international security partners as well as high priority protective programs. Specific protective actions are developed through the sector planning process and specified in SSPs;
- Implementing current agreements that affect CI/KR protection; and
- Addressing cross-sector and global issues such as cybersecurity and foreign investment.

International CI/KR protection activities require coordination with the Department of State and must be designed and implemented to benefit the Nation and its international security partners.

4.1.5.1 Cooperation with International Security Partners

DHS will work with the Department of State, international partners, and other entities involved in the international aspects of CI/KR protection, to exchange experiences, share information and develop a cooperative environment to materially improve U.S. CI/KR protection. DHS and SSAs will work with specific countries to identify international interdependencies and vulnerabilities and through international organizations such as the G8 the North Atlantic Treaty Organization (NATO), the European Union, the Organization of American States and the Organization for Economic Cooperation and Development (OECD) to enhance CI/KR protection.

While SSAs and owners and operators have responsibility for developing protective programs to address risks that arise from international factors, DHS manages specific programs to enhance the cooperation and coordination needed to address the unique challenges and opportunities posed by the international aspects of CI/KR protection:

- **International Outreach Program:** DHS, in cooperation with the Department of State and other Federal agencies, carries out international outreach activities to engage foreign countries and international/multinational organizations to promote a global culture of physical and cybersecurity. The

1 outreach activities enable international cooperation and engage constituencies that do not traditionally
2 address CI/KR protection and security. This outreach encourages the development and adoption of
3 best practices, training, and other programs, which improve the protection of U.S. CI/KR overseas, and
4 the reliability of international CI/KR on which this country depends.

- 5 • **National Cyber Exercises:** DHS and its security partners conduct exercises to identify, test, and
6 improve coordination of the cyber incident response community, including Federal, State, local, tribal,
7 regional, and international government elements, as well as private sector corporations and
8 coordinating councils.
- 9 • **The National Exercise Program:** DHS provides overarching coordination for the National Exercise
10 Program to ensure the Nation's readiness to respond in an all-hazards environment and to test the
11 steady-state protection plans and programs put in place by the NIPP. The exercise program, as
12 appropriate, engages international partners to address cooperation and cross-border issues including
13 those relating to CI/KR protection. DHS and other security partners also participate in exercises
14 sponsored by international partners.

15 **4.1.5.2 Implementing Current Agreements**

16 Existing agreements with international security partners include bilateral and multi-lateral partnerships. The
17 key partners included in existing agreements include:

- 18 • **Canada and Mexico:** The CI/KR relations between the United States and its immediate neighbors
19 make the borders virtually transparent. Electricity, natural gas, oil, roads, rail, food, water, minerals and
20 finished products flow both ways across the borders. The importance of this trade, and the
21 infrastructures that support it, was highlighted after the terrorist attacks of September 11, 2001 nearly
22 closed both borders. The United States entered into the 2001 Smart Border Declaration with Canada
23 and 2002 Border Partnership Declaration with Mexico, in part, to address bilateral CI/KR issues. In
24 addition, the 2005 Security and Prosperity Partnership of North America (SPP) established a common
25 approach to security to protect North America from external threats, prevent and respond to threats
26 within North America, and further streamline the secure and efficient movement of legitimate, low-risk
27 traffic across the shared borders.
- 28 • **United Kingdom:** DHS has formed a Joint Contact Group with the United Kingdom that brings officials
29 into regular, formal contact to discuss and resolve a range of bilateral homeland security issues.
- 30 • **G8:** The G8 has underscored its determination to combat all forms of terrorism and to strengthen
31 international cooperation. The G8 heads of government attending the July, 2005 meeting in Scotland,
32 issued a Statement on Counter-Terrorism citing three areas of focus for the G8 that relate to CI/KR
33 protection:
 - 34 ➤ To improve the sharing of information on the movement of terrorists across international borders;
 - 35 ➤ To assess and address the threat to the transportation infrastructure; and
 - 36 ➤ To promote best practices for rail and metro security.
- 37 • **NATO:** NATO addresses CI/KR protection issues through the Senior Civil Emergency Planning
38 Committee (SCEPC), the senior policy and advisory body to the North Atlantic Council on civil
39 emergency planning and disaster relief matters. The Committee is responsible for policy direction and

1 coordination of Planning Boards and Committees in the NATO environment. It has developed
2 considerable expertise that applies to CI/KR protection and has planning boards and committees
3 covering Ocean Shipping, Inland Surface Transport, Civil Aviation, Food and Agriculture, Industrial
4 Preparedness, Civil Communications Planning, Civil Protection, Civil-Military Medical Issues.

5 **4.1.5.3 Approach to International Cybersecurity**

6 International cooperation in cybersecurity helps to foster national and international activities that promote a
7 global culture of security and improve the Nation's overall incident preparedness and response posture.
8 The U.S. government proactively integrates its intelligence capabilities to protect the country from cyber
9 attack; its diplomatic outreach and advocacy and operational capabilities to build awareness,
10 preparedness, capacity, and partnerships in the global community; and its law enforcement capabilities to
11 combat cyber crime wherever it originates. These efforts require interaction between policy and operational
12 functions to coordinate national and international activity that is mutually supportive across the globe:

- 13 • **International Cybersecurity Policy:** The United States is working with key allies on cybersecurity
14 strategic policy and operational cooperation. Leveraging pre-existing relationships among Computer
15 Security Incident Response Teams (CSIRTs), DHS has established a preliminary framework for
16 cooperation on cybersecurity policy, watch and warning, and incident response with key allies such as
17 Australia, Canada, New Zealand, and the United Kingdom. This framework recognizes ongoing
18 international cyber incident management activities conducted as collaborative efforts involving internet
19 service providers and multinational corporations with involvement from government law enforcement
20 and other organizations.
- 21 • **Multilateral Frameworks:** The U.S. government uses existing multilateral frameworks and newly
22 forming bilateral dialogues to encourage countries to identify key cybersecurity points-of-contact and
23 develop computer security incident response teams. The Asia Pacific Economic Cooperation (APEC)
24 Telecommunications and Information Working Group, for example, has engaged in a capacity-building
25 program to help member countries develop computer emergency response teams. Several countries in
26 the region participate in the Asia Pacific Computer Emergency Response Team (APCERT). The U.S.
27 outreach strategy for comprehensive cyber laws and procedures draws on the Council of Europe
28 Convention on Cyber crime, the G8 High Tech Crime Working Group principles for fighting cyber crime
29 and protecting critical information infrastructure, the OECD guidelines on information and network
30 security, and United Nations General Assembly resolutions based on the G8 and OECD effort.
- 31 • **Regional Groups:** DHS, in cooperation with the Department of State, provides leadership in regional
32 forums, such as the Organization of American States (OAS) and APEC, to raise awareness and
33 develop cooperative programs on cybersecurity. The OAS has approved a framework proposal by its
34 Cybersecurity Working Group to create an OAS regional computer incident response network that
35 includes information sharing and capacity building.

36 **4.1.5.4 Foreign Investment in CI/KR**

37 CI/KR protection may be affected by foreign investment and ownership of sector assets. This issue is
38 monitored at the Federal level by the Committee on Foreign Investment in the United States and, in some
39 cases, the Federal Communications Commission. Membership of the Committee includes the Secretaries
40 of State, Defense, Commerce, Energy and Homeland Security; the Attorney General; the Director of the

Office of Management and Budget; the U.S. Trade Representative; and the Chairman of the Council of Economic Advisers, and is chaired by the Secretary of the Treasury. The Committee provides a forum for assessing the impacts of proposed foreign investments on CI/KR protection, government monitoring activities aimed at ensuring compliance with agreements that result from CFIUS rulings, and supporting executive branch reviews of applications to the Federal Communications Commission from foreign entities to assess if they pose any threat to CI/KR.

4.2 Information-Sharing: A Networked Approach

Information sharing is both a critical component and a net result of establishing effective security partnerships. When owners and operators are provided with a comprehensive picture of threats and participate in ongoing two-way information flow, their ability to assess risks, make prudent security investments, and take protective actions is substantially enhanced. Similarly, when government is equipped with a solid understanding of private sector information needs and requirements, it can adjust its information collection, analysis, synthesis, and dissemination activities accordingly.

Efficient information-sharing mechanisms and processes are required for the implementation of effective, coordinated, and integrated CI/KR protective actions. The NIPP information-sharing approach constitutes a shift from a strictly hierarchical to a networked model, allowing movement of information both vertically and horizontally, as well as the ability to enable decentralized decision making and actions. The objectives of the networked approach are to:

- Enable secure multi-directional information sharing between and across government and industry that reduces redundant reporting requirements to the greatest extent possible;
- Implement a common set of communication, coordination, and information-sharing capabilities for all security partners;
- Provide asset owners and operators with a robust communications framework tailored to their specific information sharing requirements, risk landscape, and protective architecture;
- Provide security partners with a comprehensive threat assessment picture that includes general and specific threats, incidents and events, impact assessments, and best practices;
- Maximize the flow of information required for security partners to assess risks, conduct risk management activities, invest in security measures, and allocate resources; and
- Protect the integrity and sensitivity of shared information.

The information-sharing process is designed to communicate both specific threats and information pertaining to the general threat environment (e.g., plausible threats, vulnerabilities, potential consequences) so that owners and operators can assess risks, make appropriate security investments, and take effective and efficient protective actions.

4.2.1 The Homeland Security Information Network

Figure 4-2 provides a simplified illustration of the broad concept of the NIPP multi-directional networked information-sharing approach. The information-sharing network consists of components that are connected by a national Web-based communications platform, known as the Homeland Security Information Network

(HSIN), so that security partners can obtain, analyze, and share information. The diagram illustrates how the HSIN is used to provide a platform for two-way and multi-directional information sharing between and among DHS; the Federal intelligence community; Federal departments and agencies with CI/KR protection responsibility; State, local, and tribal jurisdictions; and the private sector. These security partners are grouped into nodes in the information-sharing network approach.

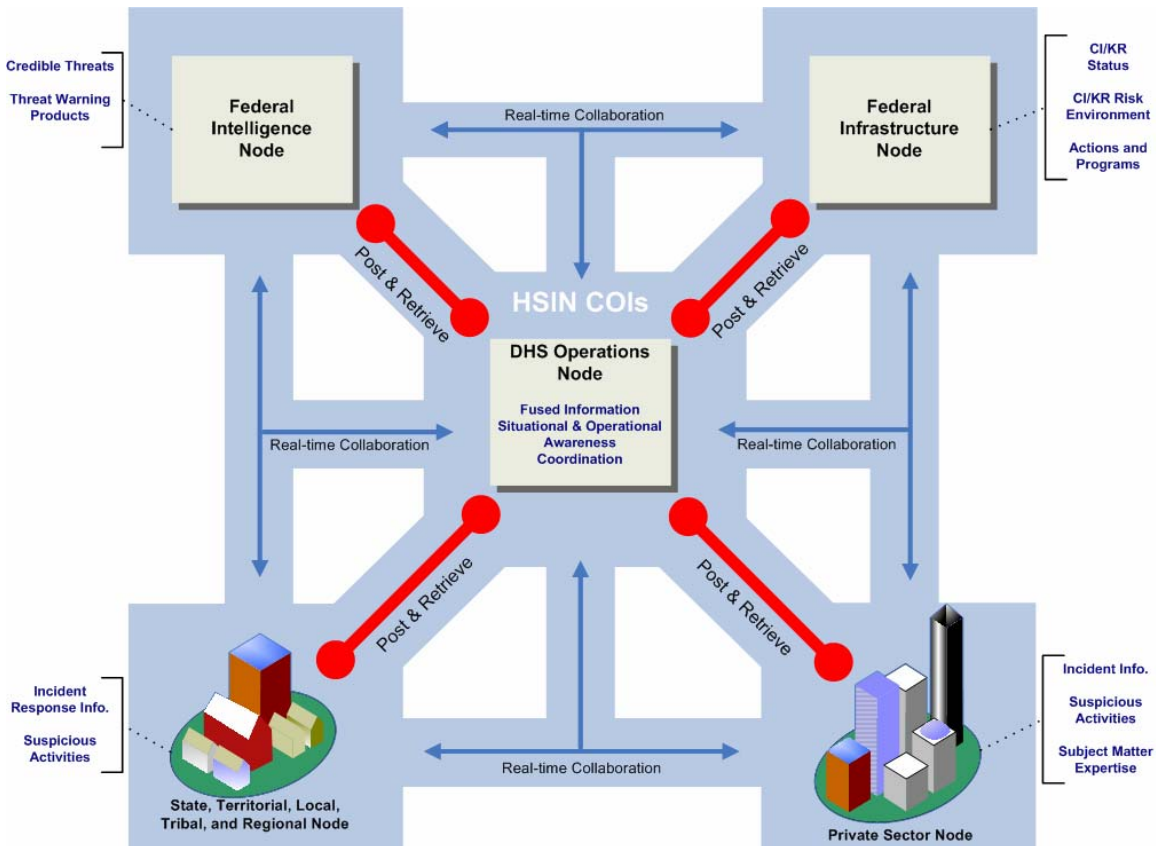


Figure 4-2: NIPP Information-Sharing Approach

When fully deployed, the HSIN will constitute a robust and significant information-sharing enabler. The linkage of the nodes will result in a dynamic view of the total threat and risk landscape. However, it is important to note that the HSIN is not the only available mechanism for DHS and security partners to share information. Other supporting technologies and more traditional methods of communication, both classified and unclassified, will continue to be employed for CI/KR protection, as appropriate, and fully integrated into the network approach.

DHS works with security partners to measure the efficacy of the network and to identify areas in which new mechanisms or supporting technologies are required. The HSIN and the nodes of the NIPP information-sharing approach are detailed in the subsequent sections. The HSIN serves as the secure platform that enables security partners to collaborate and share information with each other and DHS. By offering a user-friendly, efficient conduit for information sharing, HSIN enhances the combined effectiveness of all security partners in an all-hazards environment.

1 The HSIN is composed of multiple, non-hierarchical Communities of Interest (COIs) that offer security
 2 partners the means to post and retrieve important documents, based on secure access. This structure
 3 allows government and industry partners to engage in collaborative exchanges, based on specific
 4 information and security requirements, mission emphasis, or interest level. Table 4-1 provides a brief
 5 description of the currently available HSIN COIs. Each COI establishes participant screening, vetting, and
 6 verification processes that are appropriate for the sector CI/KR landscape and requirements for information
 7 protection. For example in some sectors applicants are vetted through the SCC; others may require
 8 participants to be documented members of a specific profession such as law enforcement; while others
 9 may require the completion and verification of a detailed application form.

Table 4-1: Currently Available HSIN COI

COI	Description
Counterterrorism (HSIN-CT)	Enables Federal, State, local, or tribal government agencies to share information relating to counterterrorism and incident management.
Critical Infrastructure Warning Information Network (CWIN)	A network within HSIN that provides mission-critical, survivable connectivity for DHS, SSAs, HSAs, Emergency Operations Centers (EOCs), and private sector entities vital to restoring the Nation's CI/KR.
Critical Sector (HSIN-CS)	A collection of portals established by the DHS/OIP to support and encourage information sharing and collaboration by the private sector within each CI/KR sector, across the sectors, and between the sectors and the government.
Emergency Management (HSIN-EM)	Enables information sharing between emergency management personnel at the Federal, State, local, and tribal levels, including EOCs.
Intelligence	Enables information sharing between authorized users in the intelligence community. Initially being used as a DHS/OI&A Intranet.
International	Enables information sharing between international partners requiring close coordination with the Homeland Security Operations Center (HSOC).
Law Enforcement (HSIN-LE)	Enables information sharing between all Federal, State, local, and tribal departments requiring access to Law Enforcement Sensitive information. COI members must meet the Department of Justice definition of law enforcement.
Law Enforcement–Analysis (JRIES LE-A)	Enables information sharing between law enforcement departments that have major Intelligence centers and are approved by the Joint Regional Information Exchange System (JRIES) Board.
Other COIs	HSIN provides the capability to develop additional temporary or permanent COIs on an as-needed basis. Examples include HSIN National Special Security Events (NSSE) ⁹ and HSIN National Capital Region (NCR).
Secret Network	An interim capability ¹⁰ that is used to communicate Secret-level information to State EOCs and select police departments.
US-CERT (HSIN-US-CERT)	A focal point for communicating and addressing cybersecurity incidents and other relevant cyber information within the Federal government.
US Public, Private, Partnership (US P3)	Designed, implemented, and deployed as a regionally coordinated private and public information exchange and alerting forum.

⁹ An event which, because of its size, as well as its national political, social, and/or symbolic significance, has been deemed by the Department of Homeland Security to face a significantly heightened risk of terrorism or criminal activity and warrants coordinated Federal security oversight.

¹⁰ A new DHS backbone, known as the Homeland Security Data Network (HSDN), is being implemented to securely communicate classified information to all Federal, State, local, and tribal agencies capable of receiving Secret-level information.

4.2.2 The Federal Intelligence Node

The Federal Intelligence Node, comprised of national Intelligence Community (IC) agencies and the DHS Office of Intelligence and Analysis (DHS/OI&A), identifies and establishes the credibility of general and specific threats. DHS/OI&A analyzes and validates, to the greatest degree possible, information received and works closely with components of the Federal Infrastructure Node to generate and disseminate threat warning products to security partners, both internal and external to the network, as appropriate.

As specified in the National Intelligence Strategy, the IC works to create an information-sharing environment in which access to terrorism information is matched to the roles, responsibilities, and missions of all organizations engaged in countering terrorism, and is timely, accessible, and relevant to their needs.

4.2.3 The Federal Infrastructure Node

The Federal Infrastructure Node, comprised of SSAs, other Federal departments and agencies, and DHS/OIP, gathers and receives infrastructure incident/event information from a variety of sources to assess the actual or potential status of CI/KR. Based on these assessments and in coordination with CI/KR owners and operators, recommendations on protective actions are developed and made available to the appropriate security partners.

Within the DHS/OIP, the HITRAC is responsible for fusing credible, multi-source threat information received from the DHS/OI&A with incident/event impact assessments and vulnerability information provided by DHS/OIP. Once the information is fused, HITRAC passes its analytical products to both DHS/OI&A and DHS/OIP to enable situational awareness, additional analysis, or the generation of threat warning products for dissemination to a wide range of security partners. This provides a real-time assessment of the CI/KR risk environment.

4.2.4 State, Local, Tribal, and Regional Node

This node provides vital links between DHS and security partners at the State, local, regional and tribal levels. Several established communications channels provide protocols for passing information from the local to State to Federal level. The NIPP networked approach augments these established communications channels by providing the ability to engage in two-way information sharing directly with the Federal government, as warranted. Members of this node provide incident response and first-responder information, and reports of suspicious activity to the FBI and HSOC for awareness and analysis. HSAs receive and further disseminate DHS-originated threat warning products, as appropriate.

Several States have also established fusion centers to facilitate a collaborative process between law enforcement, public safety, and private entities to collect, integrate, evaluate, analyze, and disseminate criminal intelligence and other information. Additionally, DHS Protective Security Advisors (PSAs) assist efforts to identify, assess, monitor, and minimize risk to CI/KR at the regional or local level. PSAs facilitate, coordinate, and/or perform vulnerability assessments for local CI/KR, and assist with security efforts coordinated by HSAs, as requested.

4.2.5 Private Sector Node

The Private Sector Node includes CI/KR owners and operators, SCCs, ISACs, and trade associations that provide incident information, event information, and reports of suspicious activity that may indicate actual or potential terrorist intent. DHS, in return, provides threat warning products, protective strategies, and alert notification to a variety of industry coordination and information-sharing mechanisms, and directly to affected CI/KR owners and operators.

The NIPP networked approach connects and augments existing information-sharing mechanisms, where appropriate, to reach the widest possible population of infrastructure owners and operators. Owners and operators need accurate and timely incident and threat-related information in order to effectively manage risk, and make decisions regarding protective strategies, partnerships, mitigation plans, security measures, and investments for addressing the risks.

ISACs are an example of an effective private sector information-sharing mechanism. Originally established by Presidential Decision Directive 63 (PDD-63) in 1998, ISACs are sector-specific entities that advance physical and cyber CI/KR protection efforts by establishing and maintaining frameworks for interaction between and among members and external security partners. ISACs typically serve as the tactical and operational arms of sector information-sharing efforts. ISAC functions include, but are not limited to: supporting sector-specific information/intelligence requirements for incidents, threats and vulnerabilities; providing secure capability for members to exchange and share information on cyber, physical or other threats; establishing and maintaining operational-level dialogue with appropriate governmental agencies; identifying and disseminating knowledge and best practices; and promoting education and awareness.

The sector partnership model recognizes that not all CI/KR sectors have established ISACs. Each sector has the ability to implement a tailored information-sharing solution that may include ISACs or other new and/or existing mechanisms, such as trade associations, security organizations, and industry-wide or corporate operations centers, working in concert to expand the flow of knowledge exchange to all infrastructure owners and operators. Most ISACs are members of the ISAC Council, which provides the mechanism for inter-sector sharing of operational information. Sectors that do not have ISACs per se use other mechanisms that participate in the HSIN and other CI/KR protection information sharing arrangements. For the purposes of the NIPP, these operationally oriented groups are also referred to collectively as ISACs.

ISACs vary greatly in composition (i.e., membership), scope (e.g., focus and coverage within a sector), and capabilities (e.g., 24/7 staffing and analytical capacity), as do the sectors they serve. As the sectors define and implement their unique information sharing mechanisms for CI/KR protection, the ISACs will remain an important information-sharing mechanism for many sectors.

4.2.6 DHS Operations Node

The DHS Operations Node maintains close working relationships with its government and private sector security partners to enable and coordinate a fused common operational picture, provide operational and situational awareness, and facilitate CI/KR information sharing within and across sectors. DHS Watch Operations Centers enable this real-time awareness and assessment to support CI/KR protection.

1 The principal purpose of a watch operations center is to collect and share information. Therefore, the value
2 and effectiveness of a watch operations center is largely dependent upon a timely, accurate, and extensive
3 population of information sources. The NIPP information-sharing networked approach virtually integrates
4 several primary watch operations centers to enhance information exchange with security partner operations
5 centers, providing a far-reaching network of awareness and coordination.

6 **4.2.6.1 Homeland Security Operations Center**

7 The Homeland Security Operations Center (HSOC) serves as the Nation's hub for information sharing,
8 situational awareness, and domestic incident management, increasing coordination among Federal, State,
9 local, tribal, and private sector partners, as well as select members of the international community. As such,
10 it is at the center of the NIPP information-sharing network.

11 The HSOC includes representatives from more than 35 Federal departments and agencies, of State and
12 local law enforcement, the Federal intelligence community, and other homeland security and emergency
13 management entities. Each representative contributes to the information-sharing and coordination functions
14 of the center which include:

- 15 • **Information Collection and Analysis:** The HSOC maintains national-level situational awareness and
16 provides a centralized, real-time flow of information between security partners. An HSOC Common
17 Operational Picture (COP) is generated using data collected from across the country providing a broad
18 view of the Nation's current overall threat and preparedness status. Using the COP, HSOC personnel,
19 in coordination with the FBI, perform initial assessments to gauge the terrorist nexus and track
20 operational actions taking place across the country in response to the threat. The information compiled
21 by the HSOC is accessible to appropriate security partners through the HSIN.
- 22 • **Situational Awareness and Incident Response Coordination:** The HSOC is the primary situational
23 awareness conduit for the White House Situation Room. As such, it provides information needed to
24 make decisions and define courses of action, and serves as primary information-collection and
25 reporting mechanism for the Interagency Incident Management Group (IIMG) as outlined in the NRP.¹¹
- 26 • **Threat Warning Products:** DHS jointly reviews threat information with partners in the FBI, Intelligence
27 Community, and other Federal agencies on a continuous basis. When a threat is determined to be
28 credible and actionable, DHS/OI&A is responsible for coordinating with these Federal partners during
29 the development and dissemination of threat warning products. This coordination ensures, to the
30 greatest extent possible, the accuracy and timeliness of the information, as well as concurrence by
31 Federal partners.

32 DHS disseminates three categories of threat warning products to Federal, State, local, and tribal
33 governments, as well as to private sector organizations and international partners through the HSIN,
34 established email distribution lists, and other methods, as required:

¹¹ The IIMG is a headquarters-level group comprised of senior representatives from DHS components, other Federal departments and agencies, and non-governmental organizations. The IIMG provides strategic situational awareness, synthesizes key intelligence and operational information, frames operational courses of action and policy recommendations, anticipates evolving requirements, and provides decision support to the Secretary of Homeland Security and other National authorities during periods of elevated alert and National domestic incidents.

- 1 • **Threat Advisories:** Contain actionable threat information and provide recommended protective actions
2 based on the nature of the threat. They also may communicate a change, national, regional, or sector-
3 specific, in the level of the HSAS.
- 4 • **Information Bulletins:** Communicate threat information that does not meet the timeliness, specificity,
5 or criticality criteria of an advisory but is pertinent to the security of U.S. CI/KR.
- 6 • **Homeland Security Information Messages:** Provide uncorroborated threat information focusing on
7 specific geographical targets, timing or methodology in an expedited manner. A deliberate tradeoff is
8 made to forego the time needed for corroboration and full evaluation by the Intelligence Community in
9 favor of the timeliness of dissemination.

10 4.2.6.2 National Infrastructure Coordinating Center

11 The National Infrastructure Coordinating Center (NICC) is a 24/7 watch operation center that maintains
12 operational and situational awareness of the Nation's CI/KR sectors. As an extension of the HSOC, the
13 NICC provides a centralized mechanism and process for information sharing and coordination between and
14 among government, SCCs, GCCs, and other industry partners.

15 The NICC receives situational, operational, and incident information from CI/KR sectors, in accordance with
16 information-sharing protocols established in the NRP. The NICC also disseminates a wide range of
17 products containing warning, threat, and CI/KR protection information to security partners:

- 18 • **Alerts and Warnings:** The NICC disseminates threat-related information products to an extensive
19 customer base of industry partners.
- 20 • **Suspicious Activity and Potential Threat Reporting:** The NICC receives and processes reports from
21 the private sector on suspicious activity or potential threats to the Nation's CI/KR. The NICC documents
22 the information provided, compiles additional details surrounding the suspicious activity or potential
23 threat, and disseminates the report to DHS Sector Specialists, HSOC, and the FBI.
- 24 • **Incidents and Events:** When an incident or event occurs, the NICC coordinates with DHS Sector
25 Specialists, industry partners, and other established information-sharing mechanisms to communicate
26 pertinent information. As needed, the NICC generates reports detailing the incident as well as the
27 impacted (or potentially) impacted sectors and disseminates them to the HSOC.
- 28 • **National Response Planning and Execution:** The NICC supports the NRP by facilitating information
29 sharing among SCCs, GCCs, ISACs, and other security partners during mitigation, response, and
30 recovery activities.

31 4.2.6.3 National Coordinating Center for Telecommunications

32 The National Coordinating Center for Telecommunications (NCC) is a joint industry-government entity that
33 regularly passes situational and operational information to the HSOC, NICC, and other DHS components.
34 The NCC coordinates with industry and Federal government organizations involved in National
35 Security/Emergency Preparedness (NS/EP) telecommunications services.

36 In support of the NIPP, the NCC serves as the mechanism by which the Federal government and the
37 telecommunications industry jointly respond to NS/EP telecommunications services. The NCC provides the

1 capability to rapidly exchange information and expedite NS/EP telecommunications response. While the
2 primary focus of the NCC is the NS/EP telecommunication service requirements of the Federal
3 government, the NCC also monitors the status of all essential telecommunication facilities, including public
4 switched networks.

5 **4.2.6.4 U.S. Computer Emergency Readiness Team**

6 The U.S. Computer Emergency Readiness Team (US-CERT) is a 24/7 single point of contact for
7 cyberspace analysis warning, information sharing, and incident response and recovery for security
8 partners. It is a partnership between DHS and the public and private sectors designed to enable protection
9 of the Nation's Internet infrastructure and to coordinate the prevention of, and response to, cyber attacks
10 across the Nation.

11 US-CERT coordinates with security partners to disseminate reasoned and actionable cybersecurity
12 information through a Web site, accessible via the HSIN, and through mailing lists. Among the products it
13 provides are:

- 14 • **Cybersecurity Bulletins:** Weekly bulletins written for systems administrators and other technical users
15 that summarize published information concerning new security issues and vulnerabilities.
- 16 • **Technical Cybersecurity Alerts:** Written for system administrators and experienced users, technical
17 alerts provide timely information on current security issues, vulnerabilities, and exploits.
- 18 • **Cybersecurity Alerts:** Written in language for home, corporate, and new users, these alerts are
19 published in conjunction with technical alerts when there are security issues that affect the general
20 public.
- 21 • **Cybersecurity Tips:** Tips provide information and advice on a variety of common security topics. They
22 are published biweekly and are primarily intended for home, corporate, and new users.
- 23 • **National Web Cast Initiative:** DHS, through US-CERT, and the Multi-State ISAC has launched a joint
24 partnership to develop a series of national Web casts that will examine critical and timely cybersecurity
25 issues. The purpose of the initiative is to strengthen the Nation's cyber readiness and resilience.

26 US-CERT also provides a method for citizens, businesses, and other important institutions to communicate
27 and coordinate directly with the U.S. government on matters of cybersecurity. The private sector can use
28 the protections afforded by the Critical Infrastructure Information Act to electronically submit proprietary
29 data to US-CERT.

30 **4.2.7 Use of Other CI/KR Information-Sharing Components and Technologies**

31 DHS, other Federal agencies, and the law enforcement community use additional supporting technologies
32 to provide information to a broad range of security partners. These outreach activities include:

- 33 • **Cybercop Portal:** The DHS-sponsored Cybercop Portal is a secure Internet-based information-sharing
34 mechanism that connects more than 5,300 members of the law enforcement community worldwide
35 (including bank investigators and the network security community) involved in electronic crimes
36 investigations.

- 1 • **Web-Based Services for Citizens:** A variety of Web-based information services are available to
2 enhance the general awareness and preparedness of American citizens. These include
3 CitizenCorps.gov, FirstGov.gov, Ready.gov, and USAonwatch.org.
- 4 • **Sharing National Security Information:** The ability to share relevant classified information poses a
5 number of challenges particularly when the majority of industry facilities are neither designed for, nor
6 accredited to receive, store, and dispose of these materials. Ultimately, HSIN may be used to more
7 efficiently to share appropriate classified national security information with cleared private sector
8 owners and operators during incidents, times of heightened threat, or on an as-needed basis. While
9 supporting technologies and policies are identified to satisfy this requirement, DHS will continue to
10 expand its initiative to sponsor security clearances for designated private sector owners and operators,
11 sharing classified information using currently available methods.
- 12 • **Law Enforcement Online:** The FBI provides Law Enforcement Online (LEO) as national focal point for
13 electronic communication, education, and information sharing capability for the law enforcement
14 community. LEO, which can be accessed by any approved employee of a local, State, or Federal law
15 enforcement agency, or approved member of an authorized law enforcement special interest group, is
16 intended to provide a communication mechanism to link all levels of law enforcement throughout the
17 United States.
- 18 • **FBI's InfraGard:** InfraGard is an information sharing and analysis effort serving the interests and
19 combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a
20 partnership between the FBI and the private sector. InfraGard is an association of businesses,
21 academic institutions, state and local law enforcement agencies, and other participants dedicated to
22 sharing information and intelligence to prevent hostile acts against the United States. InfraGard
23 Chapters are geographically linked with FBI Field Office territories. Each InfraGard Chapter has an FBI
24 Special Agent Coordinator, who works closely with Supervisory Special Agent Program Managers in
25 the Cyber Division at FBI Headquarters.
- 26 • **Interagency Cybersecurity Efforts:** Interagency cooperation and information sharing are essential to
27 improving national counterintelligence and law enforcement capabilities pertaining to cybersecurity.
28 The intelligence and law enforcement communities have various official and unofficial information-
29 sharing mechanisms in place. Examples include:
 - 30 ➤ **U.S. Secret Service's Electronic Crime Task Forces:** U.S. Secret Service's Electronic Crime
31 Task Forces (ECTFs) provide interagency coordination on cyber-based attacks and intrusions. At
32 present, 15 ECTFs are in operation, with an expansion planned.
 - 33 ➤ **FBI's Inter-Agency Coordination Cell:** The Inter-Agency Coordination Cell is a multi-agency
34 group focused on sharing law enforcement information on cyber-related investigations.
 - 35 ➤ **Computer Crime and Intellectual Property Section:** The FBI and the Secret Service meet
36 regularly to coordinate and deconflict investigations, ensuring there is no duplication of effort.

37 **4.3 Protection of Sensitive CI/KR Information**

38 NIPP implementation will rely greatly on critical infrastructure information provided by the private sector.
39 Much of this is sensitive business or security information that could cause serious damage to the economy,
40 public safety, or security if unauthorized disclosure or access to this information takes place.

The Federal government has a statutory responsibility to safeguard information collected from or about infrastructure activities. Section 203 of the Homeland Security Act requires the Secretary of DHS to “ensure that any material received pursuant to this section is protected from unauthorized disclosure and handled and used only for the performance of official duties.” DHS and other Federal agencies use a number of programs and procedures, such as the Protected Critical Infrastructure Information (PCII) Program, to ensure that CI/KR information is properly safeguarded, and that information required to implement the NIPP is solicited. In addition to PCII, other programs and procedures are used to protect sensitive information; these apply to Sensitive Security Information for transportation activities; Unclassified Controlled Nuclear Information; contractual provisions; Federal Security Classification Guidelines; and other legal guidelines.

4.3.1 Protected Critical Infrastructure Information Program

The PCII Program was established pursuant to the Critical Infrastructure Information (CII) Act of 2002. The Program provides a means for sharing private sector information with the government and while providing assurances that the information will be exempt from unauthorized public disclosure and will be properly safeguarded. This enables members of the private sector to voluntarily submit sensitive information regarding the CI/KR to DHS with the assurance that the information will be protected. Appendix 4C provides a more detailed description of the PCII Program.

4.3.1.1 PCII Program Office

DHS established the PCII Program Office to manage CII information, develop protocols for handling this information, and raising awareness of the need for protected information sharing between the public and private sectors.

The PCII Program Office is responsible for receiving, validating, and safeguarding CII submitted to DHS. The Program Office works with government programs and those entities in the private sector willing to share their information on a voluntary basis.

4.3.1.2 Critical Infrastructure Information Protection

The following process and procedures apply to all CII submissions:

- Individuals or collaborative groups may submit information for protection;
- The PCII Program Office validates that the information qualifies for protection under the Act;
- All validated PCII is stored in a secure data management system; secure methods are used for disseminating PCII;
- Authorized users must comply with safeguarding requirements defined by the PCII Program Office; and
- Any suspected disclosure of PCII will be promptly investigated. Federal employees may face significant fines or penalties for improper disclosure.

4.3.1.3 Uses of PCII

PCII may be shared with authorized government entities only for purposes of securing CI/KR and protected systems. PCII will be used for analysis, prevention, response, recovery, or reconstitution of CI/KR threatened by terrorism or other hazards.

Authorized government entities may generate advisories, alerts, and warnings relevant to the private sector based on the information provided; however, communications made available to the public must not contain any sensitive information provided by the submitter. PCII can be combined with other information, including classified information, in support of CI/KR protection activities; in such cases PCII used in such products must be marked accordingly.

4.3.1.4 PCII Protections and Authorized Users

The PCII Program has established procedures to ensure that PCII is properly accessed, used, and safeguarded throughout its lifecycle. These safeguards ensure submitted information is:

- Used appropriately for Homeland Security purposes;
- Accessed only by authorized and properly trained staff who have a need to know;
- Protected from disclosure under the Freedom of Information Act and similar State and local disclosure laws, and use in civil litigation and regulatory actions; and
- Safeguarded and handled in a secure manner.

The law and rule prescribe criminal penalties for intentional unauthorized access, distribution, and misuse of PCII:

- Federal employees may be subject to disciplinary action, including criminal and civil penalties and loss of employment;
- Contract employees may face termination and the contractor may have its contract terminated; and
- Sanctions do not apply directly to State and local officials or employees, but State and local participating entities may have their own penalties for improperly handling sensitive information and these entities may lose future access to PCII.

4.3.2 Other Security Regimes

Disclosure regimes limit the availability of information and may impose access requirements (e.g., the export control regimes that require export licenses prior to disclosure to foreign persons). Protection regimes implement safeguarding standards (e.g., the correctness of Federal budget information must be protected while it is contained in a Federal computer system, even though it is releasable to the public). Security regimes, such as those that apply to classified information and to CI/KR information, provide both protection and access restrictions.

Information need not be designated as CII in order to receive security protection and disclosure restrictions. Several other categories of information related to CI/KR require protection. Examples include, sector-

specific information such as sensitive transportation or nuclear information, or information determined to be classified information based on the analysis of unclassified information. The major categories that apply to CI/KR are discussed below.

4.3.2.1 Sensitive Security Information (SSI)

The Maritime Transportation Security Act and the Aviation Transportation Security Act establish protection for SSI. TSA and the U.S. Coast Guard may designate information as SSI when disclosure would:

- Be detrimental to security;
- Reveal trade secrets or privileged or confidential information; or
- Constitute an unwarranted invasion of privacy.

Parties accessing SSI must have the appropriate level of security clearance and a need to know. Holders of SSI must protect such information from unauthorized disclosure and must destroy the information when it is no longer needed. SSI information protection pertains to government officials as well as owners and operators of transportation activities.

4.3.2.2 Unclassified Controlled Nuclear Information (UCNI)

The Department of Defense and the Department of Energy may designate certain information as UCNI; such information relates to the production, processing, or use of nuclear material; nuclear facility design information; and security plans and measures for the physical protection of nuclear materials. This designation is used when disclosure could affect the health and safety of the public or national security by enabling illegal production or diversion of nuclear materials or weapons. Access to UCNI is restricted to those who have a need to know. Procedures are specified for marking and safeguarding UCNI.

4.3.2.3 Freedom of Information Act Exemptions and Exclusions

The Freedom of Information Act (FOIA) was enacted in 1966 and amended and modified by Congress in legislation including Electronic Freedom of Information Act of 1996 and the Privacy Act of 1974. The Act established a statutory right of public access to executive branch information in the federal government and generally provides that any person has a right, enforceable in court, to obtain access to federal agency records. Certain records may be protected from public disclosure under the act if they fall into one of three special law enforcement exclusions, which protect information such as the name of informants. They may also be protected from public disclosure under the Act if they are in one of nine exemption categories that protect such information as classified national security data, trade secrets or financial information obtained by the government from individuals, personnel and medical files, and CI/KR information.

4.3.2.4 Classified Information

Under Executive Order 12958, as amended, and Executive Order 12829, as amended, the Information Security Oversight Office of the National Archives is responsible to the President for overseeing the security classification programs in both government and industry that safeguard national security information, including information relating to defense against transnational terrorism.

Classified information is a special category of sensitive information that is accorded special protections and access controls. It has certain characteristics that distinguish it from other sensitive information. These include:

- The information can only be designated as classified by a duly empowered authority;
- The information must be owned by, produced by or for, or under the control of the U.S. government;
- The unauthorized disclosure of the information reasonably could be expected to result in identifiable damage to U.S. national security; and
- Only information relating to the following may be classified:
 - Military plans, weapons systems, or operations;
 - Foreign government information;
 - Intelligence activities (including special activities), intelligence sources or methods, or cryptology;
 - Foreign relations or foreign activities of the United States, including confidential sources;
 - Scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism;
 - U.S. government programs for safeguarding nuclear materials or facilities;
 - Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or
 - Weapons of mass destruction.

Some forms of information relating to CI/KR protection have these characteristics; this information may be determined to be classified information and protected accordingly.

4.3.2.5 Physical and Cybersecurity Measures

DHS uses strict information security protocols for the access, use, and storage of sensitive information including that related to CI/KR. These protocols include both physical security measures and cybersecurity measures. Physical security protocols for DHS facilities require access control and risk mitigation measures. Information security protocols include access controls, log-in restrictions, session tracking, and data labeling. Appendix 4C provides a discussion of these protections as applied to the NADB.

4.4 Privacy and Constitutional Freedoms

Mechanisms detailed in the NIPP are designed to provide a balance between achieving a high level of security and protecting the civil rights and liberties that form an integral part of the national character of the United States. Achieving this balance requires acceptance of some level of terrorist risk. In providing for effective protective programs, the processes outlined in the NIPP respect privacy, the freedom of expression, the freedom of movement, the freedom from unlawful discrimination, and other liberties that define the American way of life.

1 Compliance with the Privacy Act and governmental privacy regulations and procedures is a key factor
2 considered when collecting, maintaining, using, and disseminating personal information. The following DHS
3 offices support the NIPP processes:

- 4 • **DHS Privacy Office:** DHS has designated a Privacy Officer to ensure that it appropriately balances
5 mission with civil liberty and privacy concerns. The officer consults regularly with privacy advocates,
6 industry experts, and the public at large to ensure broad input and consideration of privacy issues so
7 that DHS achieves solutions that protect privacy while enhancing security.
- 8 • **DHS Office for Civil Rights and Civil Liberties:** Established to review and assess allegations of
9 abuse of civil rights or civil liberties, racial or ethnic profiling, and to provide advice on all DHS
10 components.

5. Integrating CI/KR Protection as Part of the Homeland Security Mission

This Chapter describes the linkages between the NIPP, the SSPs, and other CI/KR protection strategies, plans, and initiatives. It also describes how the unified national CI/KR protection effort integrates with the prevention, protection, response, and recovery elements of the homeland security mission.

5.1 A Coordinated National Approach to the Homeland Security Mission

The Homeland Security Act; National Strategies for Homeland Security, Physical Protection of Critical Infrastructures and Key Assets, and to Secure Cyberspace (see discussion below); a series of Homeland Security Presidential Directives; and related initiatives work together to provide the basis for a coordinated national approach to homeland security that includes a common framework for CI/KR protection, preparedness, and incident management. Figure 5-1 illustrates the relationships that, together, result in a holistic approach to homeland security.

5.1.1 Legislation

The Homeland Security Act of 2002 (Figure 5-1, Column 1) provides the primary authority for the overall homeland security mission and establishes the basis for the NIPP, the SSPs, and related CI/KR protection efforts and activities.

5.1.2 Strategies

The National Strategies for Homeland Security, the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, and the National Strategy to Secure Cyberspace, together provide the vision and direction for the CI/KR protection elements of the homeland security mission (see Figure 5-1, Column 2).

5.1.2.1 The National Strategy for Homeland Security

The President's National Strategy for Homeland Security established protection of America's CI/KR as a core homeland security mission and as a key element of the comprehensive approach to homeland security and domestic incident management. This Strategy articulated the vision for a unified "American Infrastructure Protection effort" to "ensure we address vulnerabilities that involve more than one infrastructure sector or require action by more than one agency," and to "assess threats and vulnerabilities comprehensively across all infrastructure sectors to ensure we reduce the overall risk to the country, instead of inadvertently shifting risk from one potential set of targets to another."

The strategy called for the development of "interconnected and complementary homeland security systems that are reinforcing rather than duplicative, and that ensure essential requirements are met, [and would] provide a framework to align the resources of the Federal budget directly to the task of securing the homeland."

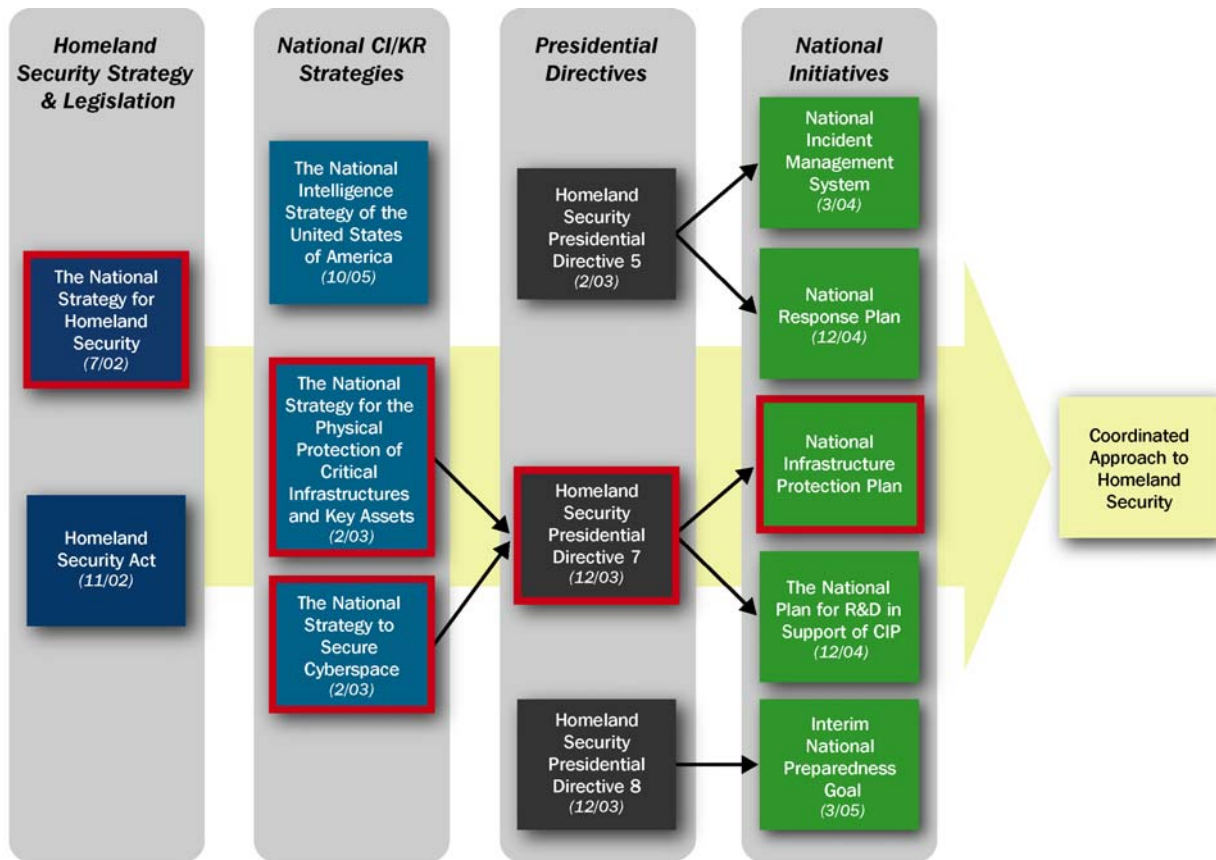


Figure 5-1: National Framework for Homeland Security

5.1.2.2 The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets identifies national policy, goals, objectives, and principles needed to “secure the infrastructures and assets vital to national security, governance, public health and safety, economy, and public confidence.” The strategy identifies specific initiatives to drive near-term national protection priorities and inform the resource allocation process; identifies key initiatives needed to secure each of the CI/KR sectors; and addresses specific cross-sector security priorities. Additionally, it establishes a foundation for building and fostering the cooperative environment in which government, industry, and private citizens can carry out their respective protection responsibilities more effectively and efficiently.

5.1.2.3 The National Strategy to Secure Cyberspace

The National Strategy to Secure Cyberspace set forth objectives and specific actions needed to prevent cyber attacks against America’s CI/KR, reduce nationally identified vulnerabilities, and minimize damage and recovery time from cyber attacks. This Strategy articulates five national priorities, including the establishment of a security response system, a threat and vulnerability reduction program, an awareness and training program, efforts to secure governments’ cyberspace, and international cooperation.

5.1.2.4 The National Intelligence Strategy of the United States of America

The National Intelligence Strategy of the United States of America outlines the fundamental values, priorities, and orientation of the Intelligence Community. As directed by the Director of National Intelligence, the strategy outlines the specific mission objectives which relate to efforts to predict, penetrate, and pre-empt threats to national security. To accomplish this, the efforts of the different enterprises of the Intelligence Community are integrated through policy, doctrine, and technology and by ensuring that intelligence efforts are appropriately coordinated with the nation's homeland security mission.

Priority in this Strategy is focused on improving the national response to cyber incidents; reducing threats from, and vulnerabilities to, cyber attacks; preventing cyber attacks that could affect national security assets; and improving the international management of, and response to, such attacks.

5.1.3 Homeland Security Presidential Directives and National Initiatives

Homeland Security Presidential Directives set national policies and executive mandates for specific programs and activities (see Figure 5-1, Column 3). The first was issued on October 29, 2001, shortly after the attacks on September 11, 2001, establishing the Homeland Security Council. It was followed by a series of directives regarding the full spectrum of actions required to "prevent terrorist attacks within the United States; reduce America's vulnerability to terrorism, major disasters, and other emergencies; and minimize the damage and recover from attacks that do occur." This section addresses the Homeland Security Presidential Directives that are most relevant to the overarching CI/KR protection component of the homeland security mission (e.g., HSPDs 3, 5, 7, and 8).

HSPD-3, Homeland Security Advisory System, provides the requirement for the dissemination of information regarding terrorist acts to Federal, State, and local authorities, and the American people. HSPD-5 addresses the national approach to domestic incident management; HSPD-7 focuses on the CI/KR protection mission; and HSPD-8 focuses on ensuring the optimal level of preparedness to protect, prevent, respond to, and recover from terrorist attacks and the full range of natural and man-made hazards. Others, such as HSPD-9, Defense of the United States Agriculture and Food, and HSPD-10, Biodefense for the 21st Century, are relevant to CI/KR protection and will be addressed in greater detail in the appropriate SSPs.

5.1.3.1 HSPD-3, Homeland Security Advisory System

HSPD-3 (March 2002) established the policy for the creation of the HSAS to provide warnings to Federal, State, and local authorities, and the American people in the form of a set of graduated "Threat Conditions" that escalate as the risk of the threat increases. At each threat level, Federal departments and agencies are required to implement a corresponding set of "protective measures" to further reduce vulnerability or increase response capabilities during a period of heightened alert. The threat conditions serve as a guidepost for the implementation of protective measures by State, local, and private sector security partners.

5.1.3.2 HSPD-5, Management of Domestic Incidents

HSPD-5 (February 2003) required DHS to lead a coordinated national effort with other Federal departments and agencies; State, local, and tribal governments; and the private sector to develop and implement a NIMS and the NRP (see Figure 5-1, Column 4).

The NIMS (March 2004) provides a nationwide template enabling Federal, State, local, and tribal governments; the private sector; and non-governmental organizations to work together effectively and efficiently to prevent, prepare for, respond to, and recover from incidents regardless of cause, size, and complexity. The NIMS provides a uniform doctrine for command and management, including the Incident Command, Multiagency Coordination, and Joint Information Systems; resource, communication, and information management; and application of supporting technologies.

The NRP (December 2004) was built on the NIMS template, signed by 29 Federal departments and agencies and three non-governmental organizations, and fully implemented on April 14, 2005. It establishes a single, comprehensive framework for the management of high-impact domestic events, termed "Incidents of National Significance," that require DHS coordination and effective response by an appropriate combination of Federal, State, local, and tribal governments; the private sector; and non-governmental organizations.

5.1.3.3 HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection

HSPD-7 (December 2003) established the U.S. policy for "enhancing protection of the Nation's CI/KR." It mandated development of the NIPP as the primary vehicle for implementing the CI/KR protection policy. HSPD-7 directed the Secretary of Homeland Security to lead development of the Plan, including, but not limited to, the following four key elements:

- A strategy to identify and coordinate the protection of CI/KR;
- A summary of activities to be undertaken to prioritize, reduce the vulnerability of, and coordinate protection of CI/KR;
- A summary of initiatives for sharing information, and for providing threat and warning data to State, local, and tribal governments and the private sector; and
- Coordination and integration, as appropriate, with other Federal emergency management and preparedness activities, including the NRP and guidance provided in the National Preparedness Goal.

The NIPP is supported by a series of SSPs, developed by the SSAs in coordination with their public and private sector security partners that detail the approach to CI/KR protection goals, initiatives, processes, and requirements for each sector.

5.1.3.4 HSPD-8, National Preparedness

HSPD-8 (December 2003) mandates development of a National Preparedness Goal (see Figure 5-1, Column 4) aimed at helping entities at all levels of government build and maintain the capabilities to prevent, protect against, respond to, and recover from major events or Incidents of National Significance as defined in the NRP in order "to minimize the impact on lives, property, and the economy."

To do this, the Goal provides readiness targets, priorities, standards for assessments and strategies, and a system for assessing the Nation's overall level of preparedness. The Goal specifies three overarching priorities: (1) implementation of the NIMS and the NRP, (2) expansion of regional collaboration, and (3) implementation of the NIPP, and several capability-specific priorities, which include strengthening information sharing and collaborative capabilities; interoperable communications capabilities; and chemical, biological, radiological, nuclear, or explosive detection, response, and decontamination. The national priorities establish "measurable readiness priorities ... that appropriately balance the potential threat and magnitude of terrorist attacks, major disasters, and other emergencies with the resources required to prevent, respond to, and recover from them." Each of these priorities is relevant to enhancing effective implementation of the NIPP and integration of the NIPP risk management framework as a vital component of achieving the Nation's homeland security mission.

The Goal uses capabilities-based planning processes and enables Federal, State, local, and tribal entities to prioritize needs, update strategies, allocate resources, and deliver programs. The Goal references standard planning tools that are applicable to implementation of the NIPP, including the Universal Task List (UTL) and the Target Capabilities List (TCL). The UTL provides a menu of tasks from all sources that may be performed to implement CI/KR protection programs, as well those needed to respond to major incidents. The TCL provides guidance on the specific capabilities and levels of capability relevant to CI/KR protection and other areas of the homeland security mission that Federal, State, local, and tribal entities will be expected to develop and maintain. The specific capabilities and levels of capability will vary based on the risk and the needs of the different types of entities. Like the NIPP, the UTL and TCL are living documents that will be enhanced and refined over time.

5.2 The CI/KR Protection Component of the Homeland Security Mission

The result of this interrelated set of national strategies, authorities, and initiatives is a common, holistic approach to achieving the homeland security mission that includes an emphasis on preparedness across the board, and on the protection of America's CI/KR as a steady-state component of routine, day-to-day business for government and private sector security partners.

The NIPP and NRP are complementary plans that span a spectrum of prevention, protection, response, and recovery to enable this coordinated approach on a day-to-day basis and during periods of heightened threat. The NIPP and its associated SSPs establish the Nation's steady-state level of protection by helping to focus resources where investment yields the largest reduction in national risk relative to cost. The NRP addresses prevention, preparedness, response, and recovery in the context of domestic threat and incident management. The National Preparedness Goal supports implementation of both the NIPP and the NRP by establishing national priorities and guidance for building the requisite capabilities at all levels of government.

Each of the guiding elements of the homeland security mission includes specific requirements for DHS and other Federal departments and agencies to build partnerships and work in cooperation and collaboration with the private sector. This cooperation and collaboration with private sector owners and operators is specifically applicable to the CI/KR protection efforts outlined in the NIPP.

The NIPP risk management framework, sector partnership model, and information-sharing mechanisms are structured to support coordination and cooperation with private sector owners and operators while recognizing the differences between and within sectors, acknowledging the need to protect sensitive information, establishing processes for two-way information sharing, and providing for smooth transitions from steady-state measures to incident response.

5.3 Relationship of NIPP to Other CI/KR Plans and Programs

The NIPP Base Plan and Appendixes outline the overarching elements of the CI/KR protection effort that generally are applicable within and across all sectors. The SSPs are an integral component of the NIPP and exist as independent documents to address the unique perspective, risk landscape, and methodologies of each sector. Homeland Security plans and strategies at the State, local, and tribal levels of government address CI/KR protection within their respective jurisdictions, as well as coordination with various regional efforts and other external entities.

5.3.1 Sector-Specific Plans

Based on guidance from DHS, SSPs are developed by SSAs in close coordination with security partners. They provide the means by which the NIPP is implemented in a consistent manner across sectors, as well as a national framework for each sector that guides the development, implementation, and updating of State and local homeland security strategies and CI/KR protection programs.

SSPs address the unique characteristics and risk landscapes of each sector while also providing consistency for protective programs, public and private protection investments, and resources. SSPs serve to:

- Define sector security partners, authorities, roles and responsibilities, and interdependencies;
- Establish procedures for sector interaction, information sharing, coordination, and partnership;
- Establish goals and objectives, developed in collaboration with security partners, required to achieve the desired end-state protective posture for the sector;
- Identify international considerations; and
- Identify the sector-specific approach or methodology that SSAs, in coordination with DHS and other security partners, will use to conduct the following activities consistent with the NIPP framework:
 - Identify priority CI/KR within the sector, to include cyber considerations;
 - Assess risks of terrorist attack, including potential consequences, vulnerabilities, and threats;
 - Assess and prioritize assets and systems of national significance within a sector;

Sector Background & Engagement
Sector Security Goals
Identify Sector Assets
Assess Sector Risks
Normalize & Prioritize
Implement Protective Programs
Measure Progress
Plan CI/KR Protection R&D
Organize & Manage Sector Responsibilities

Figure 5-2: Sector-Specific Plan Structure

- Develop protective programs based on detailed knowledge of sector operations and risk landscape;
- Use metrics to measure and communicate program effectiveness and risk reduction within the sector; and
- Address R&D requirements and activities relevant to the sector.

The structure for the SSPs (as shown in Figure 5-2) facilitates cross-sector comparisons and coordination by DHS and other SSAs. Appendix 5A provides a more detailed discussion of SSP content. Additional background on each of the sectors is provided in Appendix 5B.

SSPs must be completed, approved, and submitted by SSAs to DHS within 180 days of issuance of the NIPP. The approval process includes a formal Executive Secretariat review for GCC member departments and agencies, as well as final approval and signature by the SSA. The SSP must include a letter of agreement signed by members of the GCC and a letter of endorsement from the SCC.

5.3.2 State, Regional, Local, and Tribal CI/KR Protection Programs

Development and implementation of a CI/KR protection program is a key component of State, local, tribal, and regional homeland security efforts. Creating and managing a CI/KR protection program for a given jurisdiction entails building an organizational structure and mechanisms for coordination between government and private sector entities that can be used to implement the NIPP risk management framework. This includes taking actions within the jurisdiction to set security goals, identify assets, systems, and networks, assess risks, prioritize CI/KR across sectors, implement protective programs, and measure the effectiveness of risk-reduction efforts. These elements form the basis of CI/KR protection programs and guide the implementation of relevant CI/KR protection-related goals and objectives outlined in State, local, and tribal homeland security strategies.

In a regional context, the NIPP risk management framework and information-sharing processes can be applied through the development of a regional framework or the use of existing regional coordinating structures. Effective regional approaches to CI/KR protection involve coordinated planning and protection, and sharing of costs and risk. Regional approaches also include exercises to bring the public and private sectors together around a shared understanding of the challenges to regional resilience; analytical tools to inform decision makers on risk and risk reduction with associated benefits and costs; and forums to enable decision makers to formulate protective measures and identify funding requirements and resources within and across sectors and jurisdictions.

State, regional, local, and tribal CI/KR protection efforts enhance implementation of the NIPP and the SSPs by providing unique geographical focus and cross-sector coordination potential. To ensure that these efforts are consistent with other CI/KR protection planning activities, the basic elements to be incorporated in these efforts are provided in Appendix 5C. The recommended elements described in the Appendix recognize the variations in governance models across the States, recognize that not all sectors are represented in each State or geographical region, and are flexible enough to reflect the different authorities, resources, and issues within each State or region.

5.3.3 Other Security Partner Plans or Programs Related to CI/KR Protection

Federal security partners should review and revise, as necessary, other plans that address elements of CI/KR protection to ensure that they support the NIPP. Examples of government plans or programs that may contain relevant prevention, security, and protective activities that relate to, or affect, CI/KR protection include plans for CI/KR and BZPPs; State, local, and tribal hazard mitigation; continuity of operations; continuity of government; environmental, health, and safety; and integrated contingency plans. Federal security partners are required to complete the review of existing plans within 90 days and complete any required revisions within 180 days of the issuance of the NIPP. Review and revision of State, local, and tribal strategies and plans should be completed in accordance with overall homeland security and grant program guidance.

Private sector owners and operators develop and maintain plans for business risk management that include steady-state security and facility protection, as well as business continuity and emergency management plans. Coordination with these planning efforts is relevant to effective implementation of the NIPP. Private sector security partners are encouraged to review and revise these plans, as needed, to align them with the NIPP sector partnership model and risk management framework, and to address the terrorist threat and other man-made and natural hazards.

5.4 CI/KR Protection and Incident Management

The NIPP and the NRP, together, provide a comprehensive, integrated approach to addressing key elements of the Nation's homeland security mission to prevent terrorist attacks, reduce vulnerabilities, and respond to incidents in an all-hazards context. The NIPP establishes the overall risk-based approach that defines the Nation's CI/KR steady-state protective posture, while the NRP and NIMS provide the overarching framework, mechanisms, and protocols required for effective and efficient domestic incident management. The NIPP risk management framework, information-sharing network, and sector partnership model provide vital functions that, in turn, inform and enable incident management decisions and activities.

5.4.1 The National Response Plan

The NRP provides an all-disciplines and all-hazards approach that incorporates best practices from a wide variety of disciplines, including fire, rescue, emergency management, law enforcement, public works, and emergency medical services. The operational and resource coordinating structures described in the NRP are designed to support decision making during the response to a specific threat or incident, and serve to unify and enhance the incident management capabilities and resources of individual agencies and organizations acting under their own authority. The NRP applies to Incidents of National Significance including natural disasters, terrorist threats and incidents, and other emergencies that require overall DHS coordination.

The NRP Base Plan and annexes provide protocols for coordination among various Federal departments and agencies; State, local, and tribal governments; and private sector partners both for pre-incident prevention and preparedness, and post-incident response, recovery, and mitigation. The NRP specifies incident management roles and responsibilities, including Emergency Support Functions designed to expedite the flow of resources and program support to the incident site. SSAs, and other Federal departments and agencies have roles within the NRP structure that are distinct from their responsibilities

under the NIPP. Ongoing implementation of the NIPP risk management framework, partnerships, and information-sharing networks set the stage for CI/KR security and restoration activities within the NRP framework by providing mechanisms to quickly assess the impacts of the incident on both local and national CI/KR; assist in establishing priorities for CI/KR restoration; and augment incident-related information sharing with security partners.

5.4.2 Transitioning From NIPP Steady-State to Incident Management

Increased CI/KR steady-state protective measures corresponding to the threat levels established in the HSAS provide the bridge between routine steady-state operations using the NIPP risk management framework, and incident management activities using the NRP concept of operations for actions related to both to pre-incident prevention and post-incident response and recovery. The HSAS provides a progressive and systematic approach to match protective measures to the Nation's overall threat environment. This link between the current threat environment and the required levels of protection provides the means to transition from the steady-state processes detailed in the NIPP to the incident management processes described in the NRP.

DHS and security partners develop and implement stepped-up, steady-state protective actions to match the increased threat levels specified by the HSAS. As the elevation of HSAS threat levels require an increase in the day-to-day protective measures, the level of steady-state activities may also increase and remain in effect until the threat level changes. As the threat level increases, NRP coordinating structures are activated to enable incident management. DHS and security partners carry out their NRP responsibilities and also use the NIPP risk management framework to provide the CI/KR protection dimension needed to inform the NRP command, management, and multi-agency coordination entities. When an Incident of National Significance¹² occurs, regardless of the cause, the NRP is implemented for overall coordination of domestic incident management activities. The NIPP provides the CI/KR dimension, complementing the NRP incident management coordinating structures. Implementation of the NIPP risk management framework facilitates those actions directly related to the current threat status, incident prevention, response, restoration, and recovery.

The process for integrating CI/KR protection with incident management and transitioning from NIPP steady-state processes to NRP incident management coordination includes the following actions by DHS, SSAs, and other security partners:

- Increase protection levels to correlate with the threat level communicated through the HSAS, or in accordance with sector-specific warnings using the NIPP information-sharing networks;
- Use the NIPP information-sharing networks and risk management framework to review and establish national priorities for CI/KR protection; facilitate communication between security partners; and inform the NRP processes regarding priorities for response, recovery, and restoration of CI/KR on a national scale and within the incident area; and
- Fulfill roles and responsibilities as defined in the NRP for incident management activities.

¹² An actual or potential high-impact event that requires a coordinated and effective response by and appropriate combination of Federal, State, Territorial, tribal, local, nongovernmental, and/or private sector entities in order to save lives and minimize damage, and provide the basis for long-term community recovery and mitigation activities.

6. Ensuring an Effective, Efficient Program Over the Long Term

This Chapter addresses the efforts needed to ensure an effective, efficient CI/KR protection program over the long term. It focuses particularly on the long-lead-time elements of CI/KR protection that require stable plans and investments over time – such as generating skilled human capital, developing high-tech systems, and building public awareness. Key activities needed to enhance CI/KR protection over the long term include:

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

6.1 Building National Awareness

The development and implementation of a national awareness program for CI/KR protection was identified as a major need by the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. DHS, in conjunction with SSAs and other security partners, is responsible for developing and implementing a comprehensive national awareness program that supports the sustainability of the CI/KR protection, security investments, and public understanding of the terrorist CI/KR risk environment.

Objectives of the national awareness program are to:

- Create national awareness of the need to incorporate security considerations into business planning and operations, including employee education and training programs across all levels of government and the private sector;
- Support public and private sector decision making and enable the planning of relevant and effective protection strategies and resource allocation;
- Maintain public understanding of the evolving threat to CI/KR as assessed by the intelligence community and in the context of the HSAS; and
- Foster public confidence in efforts to address the threat environment and protection of the Nation's CI/KR.

DHS also is engaged in a comprehensive national cyberspace security awareness campaign to remove impediments to sharing vulnerability information between security partners. The campaign includes audience-specific awareness materials, expansion of the “Stay Safe Online” campaign, and development of awards programs for those in industry who make significant contributions to the effort.

6.2 Enabling Education, Training, and Exercise Programs

The NIPP establishes a framework to enable the education, training, and exercise programs that allow people and organizations to develop and maintain key CI/KR protection expertise. Building the requisite individual and organizational expertise requires initial training, attracting, and maintaining sufficient numbers of CI/KR professionals with the particular types of expertise that are unique to or are essential to CI/KR protection. This in turn requires individual education and training to develop and maintain the requisite levels of expertise through technical, formal academic and professional development programs. It also requires *organizational training and exercises* to develop the requisite organizational expertise. The framework that the NIPP establishes to enable each of these is discussed below.

6.2.1 Types of Expertise for CI/KR Protection

Some types of CI/KR protection expertise are associated with well-established disciplines that already have developed formal academic education programs, recognized technical training levels and credentials, and professional certification systems implemented through professional organizations or government licensing. Others involve unique skills and professional expertise that are specific to CI/KR protection, such as the expertise needed to implement the NIPP risk analysis and management framework. Such expertise often involves cutting-edge approaches that are not yet widely practiced and have yet to develop academic degrees or professional certification mechanisms in a nationwide system. The NIPP focuses special emphasis on the types of expertise that are unique to, or essential for, CI/KR protection; these include the skills for:

- Risk assessment and risk management;
- Cost-benefit analysis to inform risk management priorities;
- Resource allocation based on risk management priorities;
- Analysis of insider threats to CI/KR and countermeasures;
- Infrastructure dependency and interdependency analyses;
- International aspects of CI/KR protection;
- Best practices and technical capabilities for CI/KR protection;
- Best practices and technical capabilities for information sharing and protection; and
- Cybersecurity, including control systems.

6.2.2 Individual Education and Training

The NIPP recognizes the importance of leveraging existing accredited academic programs, professional certification standards, and technical training programs that are in place for the more mature and

established disciplines. Whether CI/KR protection disciplines are established or newly evolving, they must include the technical, academic, or professional skill sets on which the NIPP and SSPs are based. This requires an effort with a national scope that includes, but is not limited to, the following components:

- Technical training to provide individuals with the skills needed to perform their roles and responsibilities under the NIPP;
- Academic and research programs that result in formal degrees from accredited institutions; and
- Professional continuing education, which incorporates the latest advances in CI/KR protective approaches, and, where appropriate, certification based on government, industry, and professional society standards.

To enable each of these components, the NIPP specifies areas of emphasis that are discussed in the subsections that follow.

6.2.2.1 Technical CI/KR Protection Training

Training that is technical in nature can be grouped into two major categories: specific technical training on details of the NIPP itself for staff and decision makers; and specifics of operational activities required to detect, deter, and defend against terrorist activities for those charged with implementing CI/KR protection programs. Each are described as follows:

- **Specialized NIPP Training:** Training for managers and staff responsible for NIPP implementation should provide an awareness level of training on all aspects of the NIPP, including, but not limited to, the underlying authorities; responsibilities; risk management framework; sector partnership model; CI/KR protection program requirements; and planning, resource, and budget processes. The basic awareness level training should also provide participants with a working knowledge of how to use the NIPP and apply the principles both for steady-state CI/KR protection efforts and to enable the CI/KR protection dimension to set the stage for incident management.

DHS will provide or coordinate the development of course materials on these topics, work with security partners to facilitate the definition of general training requirements, and guide the development of national-level training standards associated with the NIPP. DHS will facilitate initial training in these topics for security partners, as appropriate.
- **Operational CI/KR Protection Training:** Technical CI/KR protection training programs for security partners enhance the knowledge and skills required to detect, deter, and defend against terrorist activities that threaten CI/KR. DHS supports and provides training resources to local law enforcement officers and others with a special focus on urban areas with significant clusters of CI/KR, localities where high-profile special events are typically scheduled, or other potentially high-risk geographical areas or jurisdictions. DHS technical training courses cover a range of operational and technical topics, such as Buffer Zone Protection Plans, workforce terrorism prevention, surveillance detection, high-risk target awareness, and weapons of mass destruction incident training.

DHS also supports cybersecurity training, education, and awareness programs by promoting more secure “out of the box” installation and use of cyber products; increasing user awareness and ease of use of the security features in products; and, where feasible, promotion of industry guides. These training efforts also implement and encourage programs that leverage the existing Cyber Corps

Scholarship for Service program, as well as various graduate and post-doctoral programs; link Federal cybersecurity and computer forensics training programs; and establish cybersecurity programs for departments and agencies, including awareness, audits, and standards.

Other Federal agencies also offer training related to CI/KR protection. For example, the Office of Personnel Management and the Department of Defense offer courses on potential CI/KR targets and protection resources, and the Department of the Treasury work with DHS to jointly provide training for criminal investigators in basic computer forensics.

DHS solicits recommendations from national professional organizations and from Federal, State, local, tribal, and private sector security partners for additional discipline-specific technical training courses related to CI/KR protection and supports course development.

6.2.2.2 Academic and Research Programs

DHS works with business graduate programs to incorporate CI/KR protection into business school programs. For example, DHS is coordinating with universities to incorporate security-related curriculum into business school programs under Project MBA, a new training program currently under development. The goal of Project MBA is to better prepare the Nation's future business leaders to plan, implement, and manage CI/KR protective programs.

DHS will examine existing cybersecurity programs within the research and academic communities to determine their applicability as models for CI/KR protection education and broad-based research. These programs include:

- Co-sponsorship of the National Centers of Academic Excellence in Information Assurance Education (CAEIAE) program with the National Security Agency (NSA); and
- Collaboration with the National Science Foundation to cosponsor the Scholarship for Service (SFS) program, also known as the Cyber Corps program. The SFS program provides grant money to selected CAEIAE and other universities with programs of a similar caliber to fund the final two years of student bachelor's, master's, or doctoral study in information assurance in exchange for an equal amount of time spent working for the Federal government.

DHS will ensure that the NCIP Protection R&D Plan appropriately considers the human capital needs for protection-related R&D by incorporating analysis of the research community's future needs for advanced degrees in protection-related disciplines into the plan development process.

6.2.2.3 Continuing Education and Professional Competency

CI/KR protection involves many skills and professions that already have developed education, training, and certification programs through professional organizations or government licensing. The CI/KR protection field also involves unique skills and professional expertise that have yet to incorporate such training and certification mechanisms into a nationwide system.

DHS encourages and, when appropriate, works with security partners to facilitate the development of continuing education, professional competency programs, and professional standards for areas requiring

unique and critical CI/KR protection expertise. For example, DHS is collaborating with the Department of Defense to guide the development of a national certification program that includes a comprehensive set of IT job skill standards for security professionals within the Federal government and private industry. DHS will encourage and, when appropriate, facilitate the development of similar professional and surety standards for the remaining areas of unique and critical CI/KR protection expertise specified above.

6.2.3 Organizational Training and Exercises

Building and maintaining organizational and sector expertise requires comprehensive exercises to test the interaction between the NIPP and the NRP for terrorist incidents, natural disasters, and other emergencies. Exercises are conducted by the private sector owners and operators, and across all levels of government; they may be organized by these entities, on a sector-specific basis, or through two major national-level programs:

- **The National Exercise Program:** DHS provides overarching coordination for the National Exercise Program to ensure the Nation's readiness to respond in an all-hazards environment and to test the steady-state protection plans and programs put in place by the NIPP and their transition to the incident management framework established in the NRP.
- **National Cyber Exercise:** DHS is conducting exercises to identify, test, and improve coordination within the cyber incident response community, including Federal, State, local, tribal, and international government elements, as well as private sector corporations and coordinating councils.

DHS and SSAs work together to ensure that these exercises include adequate testing of steady-state CI/KR protection measures and plans, including information sharing; application of the risk management framework; and the ability for a protected core of life-critical CI/KR services, such as power, food and water, and emergency transportation, to withstand attacks or natural disasters and continue to function at an appropriate level.

DHS works with other security partners to facilitate the development of national standards, guidelines, and protocols for incident management training and exercises that include CI/KR protection evaluation to ensure that exercise programs include adequate testing of CI/KR steady-state protective measures and plans.

DHS will ensure that the NIMS Integration Center, which serves as the repository and clearinghouse for reports and lessons learned from actual incidents, training, and exercises, regularly includes information on CI/KR protection best practices.

6.2.4 Security Partner Role and Approach

Given the scope and nature of the education, training, and exercise needs related to CI/KR protection, the approach adopted must, to the greatest extent possible, leverage current education, training, and exercise programs.

DHS will provide the initial training on the NIPP to introduce all security partners to the Plan's contents and requirements. DHS also encourages and, where appropriate, facilitates specialized NIPP training, professional training, continuing education, and development of professional and personnel surety

standards. It also encourages academic and research programs, and coordinates with exercise managers on the design of exercises that test the interaction between the NIPP framework and the NRP.

The interagency CI/KR Protection Training Task Force defines general training requirements and guides the development of national-level training standards associated with the NIPP. SSAs and other Federal agencies are required to review and update existing CI/KR protection-related courses to align with the NIPP. Other security partners are encouraged to review existing courses to align with the NIPP or develop courses relevant to CI/KR protection needs within their jurisdiction. All security partners should work with DHS to identify and fill gaps in current training, education, and exercise programs for those specialized disciplines that are unique to CI/KR protection.

6.3 Conducting Research and Development

In the near term, risk-based priorities address the challenge posed by the limited resources available to respond to all CI/KR protection needs by allocating protection resources where they can best reduce risk. In the longer term, R&D holds the key to more effective and cost-efficient CI/KR protection by using advances in technology. R&D programs work to improve all aspects of CI/KR protection – from detection of threats to inherently secure advanced infrastructure designs.

R&D supporting the NIPP includes planning and programs undertaken in three general areas: (1) the National Critical Infrastructure Protection R&D Plan, (2) the Federal Plan for Cybersecurity R&D, and (3) R&D efforts conducted by SSAs and other agencies in support of the requirements set forth in the President's physical and cyber CI/KR protection strategies. Additionally, Technology Pilot Programs develop solutions to CI/KR protection problems with technologies that have passed the research stage and require demonstration in operational use. Each of these is discussed in the subsections that follow. Appendix 6 provides more details on specific R&D plans and programs supporting CI/KR protection.

6.3.1 National Critical Infrastructure Protection R&D Plan

As directed by HSPD-7, the Secretary of Homeland Security works with the Director of the Office of Science and Technology Policy (OSTP), Executive Office of the President, to develop the annual National Critical Infrastructure Protection Research and Development Plan (NCIP R&D Plan) as a vehicle to support implementation of CI/KR risk management and other protection efforts.

The NCIP R&D Plan provides the focus and coordination mechanisms required to achieve the vision provided in the President's Physical and Cyber CI/KR Protection Strategies. That vision calls for a "systematic national effort to fully harness the Nation's research and development capabilities." The R&D planning process is designed to address common issues faced by the various sector security partners and ensure a coordinated R&D program that yields the greatest value across a broad range of interests and requirements. The plan addresses both physical and cyber CI/KR protection. The planning process also provides for the revision of research goals and priorities over the long term to respond to changes in threat, technology, environment, and other factors.

DHS and OSTP coordinate with Federal and private sector security partners, including academic and national laboratory representatives, during the R&D planning cycle. The interagency process used to develop and coordinate this plan is managed through the Infrastructure Subcommittee of the National

1 Science and Technology Council (NSTC), which is co-chaired by DHS and OSTP. SSAs are responsible
2 for providing input into the plan after coordination with sector representatives and experts through such
3 bodies as the SCCs and GCCs.

4 The NCIP R&D Plan articulates strategic R&D goals and identifies the R&D areas in which advances in
5 CI/KR protection must be made. The Plan also provides an R&D technology roadmap against which current
6 and planned risk management and protection R&D initiatives can be evaluated to define a program of
7 CI/KR protection-related technology development. The goals, R&D areas, and the technology roadmap of
8 the NCIP R&D Plan are discussed in the following subsections. A final subsection describes coordination of
9 SSP R&D planning with the NCIP R&D Plan.

10 **6.3.1.1 CI/KR Protection R&D Strategic Goals**

11 The NCIP R&D planning process identified three long-term, strategic R&D goals for CI/KR protection:

- 12 • A common operating picture architecture;
- 13 • A next-generation Internet architecture with “designed-in security”; and
- 14 • Resilient, self-diagnosing, self-healing systems.

15 The strategic goals are used to guide Federal R&D investment decisions and also to provide a coordinated
16 approach to the overall Federal research program. The DHS Science and Technology (S&T) Directorate
17 and OSTP will work with the Office of Management and Budget (OMB) to use the R&D Plan as a decision-
18 making tool for evaluation of budget submissions across Federal agencies. These goals also help guide
19 programs of research performers who receive Federal grants and contracts.

20 **6.3.1.2 CI/KR Protection R&D Areas**

21 R&D development projects for CI/KR protection programs fall into nine R&D areas or themes that cut
22 across all CI/KR sectors:

- 23 • Detection and Sensors Systems;
- 24 • Protection and Prevention Systems;
- 25 • Entry and Access Portals;
- 26 • Insider Threats;
- 27 • Analysis and Decision Support Systems;
- 28 • Response, Recovery, and Reconstitution Tools;
- 29 • New and Emerging Threats and Vulnerabilities;
- 30 • Advanced Infrastructure Architectures and Systems Design; and
- 31 • Human and Social Issues.

32 Organizing research in these areas enables the development of effective solutions that may be applied
33 across sectors and disciplines. These themes also provide an organizing framework for SSA use during the

development of the R&D requirements for their sectors, which will be reflected in their SSPs. These requirements specify the capabilities each sector needs to satisfy CI/KR protection needs. By incorporating these requirements into the NCIP R&D Plan, OMB is better able to ensure that agency R&D budget requests are aligned with the national R&D plan for CI/KR protection.

6.3.1.3 CI/KR Protection R&D Roadmap

The NCIP R&D technology roadmap provides a way for Federal R&D managers such as DHS, OSTP, OMB, and the SSAs to coordinate CI/KR protection R&D across the diverse set of security partners. This Roadmap provides a systematic approach to identify current technology investment plans, determine gaps, and outline the timeline for addressing unmet requirements. It also provides a systematic way to determine interrelationships among other R&D programs, both public and private, and ensures synchronization with SSA R&D plans contained in the SSPs.

6.3.1.4 Coordination of NCIP R&D Plan With SSP R&D Planning

Each SSP includes a component on sector-specific CI/KR protection R&D that explains how the sector will strengthen the linkage between sector-specific and national R&D planning efforts, technology requirements, current R&D initiatives, gaps, and candidate R&D initiatives. This component of the SSP explains the process for:

- **Sector Technology Requirements:** Identifying and providing a summary of sector technology requirements, and communicating them to the DHS S&T Directorate/OSTP for inclusion in the NCIP R&D Plan on an annual basis;
- **Current R&D Initiatives:** Annually soliciting a listing of current Federal R&D initiatives from the DHS S&T Directorate/OSTP that have the potential to meet sector CI/KR protection challenges, and providing a description of how this listing will be analyzed to indicate which initiatives have the greatest potential for a positive impact;
- **Gaps:** Conducting an analysis of the gaps between the sector's technology needs and current R&D initiatives from the DHS S&T Directorate/OSTP; and
- **Candidate R&D Initiatives:** Determining which candidate R&D initiatives are most relevant for the sector and how these will be summarized.

Each SSA will coordinate the development of the sector R&D planning component of their SSP so that these documents reflect the SSA's sector-level R&D investment priorities. Coordination between DHS/S&T and the sectors through the SSAs, GCCs and SCCs ensures that the R&D information in the SSP will be consistently documented and prioritized.

6.3.2 Cybersecurity R&D Planning

The Cybersecurity R&D Act authorized a multi-year effort to create more secure cyber technologies, to expand cybersecurity R&D, and to improve the cybersecurity workforce. To further address cyber R&D needs, OSTP has established the Cybersecurity and Information Assurance Interagency Working Group (CSIA IWG) under the NSTC. The CSIA IWG is jointly chartered by NSTC's Subcommittee on Networking and Information Technology Research and Development (NITRD) and the Subcommittee on Infrastructure.

The Director of Cybersecurity R&D in the DHS S&T Directorate co-chairs this interagency working group, which includes participation by Federal departments and agencies, as well as offices in the White House. The interagency working group coordinates policy, programs, and budgets for cybersecurity and information assurance R&D.

The CSIA IWG develops the Federal Plan for Cybersecurity R&D, which includes near-term, mid-term, and longer term cybersecurity research efforts, as called for in the National Strategy to Secure Cyberspace and as directed in HSPD-7. Specific research efforts include programs to improve the security of fundamental protocols (such as Internet Protocol Version 6) and authentication technologies.

DHS identifies critical cyber R&D requirements for incorporation into this National R&D planning effort. DHS and OSTP also facilitate communication between the public and private research communities and the security community to ensure that emerging technologies are periodically reviewed by the appropriate body within the NSTC to determine possible homeland security and cybersecurity applications or appropriateness for inclusion in the Federal research portfolio.

6.3.3 Other R&D That Supports CI/KR Protection

Other R&D efforts that support CI/KR protection are conducted by SSAs and other Federal agencies. These programs address the research requirements set forth in the President's Physical and Cybersecurity CI/KR Protection Strategies, which call for:

- Ensuring the compatibility of communications systems with interoperability standards;
- Exploring methods to authenticate and verify personal identity;
- Coordinating the development of CI/KR protection consensus standards; and
- Improving technical surveillance, monitoring, and detection capabilities.

Examples of this R&D include the SAFECOM program conducted by the DHS S&T Directorate Office for Interoperability. This program serves as the Federal umbrella to promote and coordinate initiatives between State, local, and tribal entities to develop interoperable wireless communications. SAFECOM's primary role is to work with Federal agencies and public safety personnel to define requirements and to create standards, models, and solutions to help meet those requirements.

DHS also conducts cooperative R&D programs with other Federal agencies relating to authentication and verification of personal identity for the CI/KR protection workforce and works with the American National Standards Institute (ANSI) and the National Institute of Standards and Technology (NIST) through the Homeland Security Standards Panel (HSSP) to help coordinate the development of consensus standards that support CI/KR protection.

6.3.4 Technology Pilot Programs

DHS identifies CI/KR protection needs common to certain types of assets or to geographical areas while conducting site assistance, buffer zone protection visits, and other vulnerability and risk assessments. In some situations, a technological solution may be the best approach to addressing such needs. If a development program is required to create or test a potential technological solution, the DHS S&T

Directorate works closely with relevant security partners to implement a technology pilot program. In some cases, this involves working with the DHS Office of Grants and Training (G&T) to identify funds and specialized training. If the pilot program is successful, the technological solutions are then implemented in other locations where similar needs exist. Three of the first technology pilot programs provide good examples of the capabilities that these programs can offer security partners:

- **The National Capital Region Rail Security Corridor Pilot Project:** This project is designed to address security challenges surrounding high-risk rail infrastructure and freight traffic transiting major urban areas while maintaining fluid rail operations and meeting the needs of local law enforcement, first-responders, and the Federal government.
- **The Constellation Automated Critical Asset Management System:** This project is being developed through a partnership between DHS and the City and County of Los Angeles. It includes a complete reporting capability to answer both local and national data calls on infrastructure, including information on location, size, key contacts, types of hazardous materials on site, and vulnerability assessments. It also provides for the automatic generation of BZPPs and pre-incident operational plans for local police and first-responder use in real time.
- **The South Florida Coastal Surveillance Prototype Test Bed:** This project is a joint effort between the DHS S&T Directorate and the U.S. Coast Guard (USCG) designed to provide an advanced port and coastal surveillance system in the Port Everglades, Miami, and Key West areas.

6.4 Building and Maintaining Databases, Simulations, and Other Tools

Many data systems, databases, models, simulations, decision support systems, and similar information tools currently exist or are under development to enable the execution of national risk management for CI/KR.

To keep pace with the constantly evolving threat, technology, and business environments, these tools must be updated and, in some cases, new tools must be developed. Priority efforts in this area will be focused on updating and improving key databases, developing and maintaining simulation and modeling capabilities, and coordinating with security partners on databases and modeling.

6.4.1 National CI/KR Protection Data Systems

HSPD-7 directs the Secretary of Homeland Security to implement plans and programs that identify, catalog, prioritize, and protect infrastructure in cooperation with all levels of government and private sector entities. Data systems currently provide the capability to catalog, prioritize, and protect CI/KR through such functions as:

- Maintaining an inventory of asset information and estimating the potential consequences of an attack or incident (e.g., the National Asset Database);
- Storing information related to terrorist attacks or incidents (e.g., the National Threat Incident Database);
- Analyzing dependencies and interdependencies (e.g., the Critical Infrastructure Protection Decision Support System);

- Managing the implementation of various protective programs (e.g., the BZPP Request Database); and
- Providing the continuous maintenance and update required to enable data in these systems to reflect changes in actual circumstances.

Properly maintaining systems with current and useful data involves long-term support, coordination, and resource commitments by DHS, the SSAs, the States, private sector entities, and other security partners. Important aspects of the support, coordination, and resource commitments required over the long term to sustain the NIPP include:

- **Need for Information Protection:** Data accuracy and currency for CI/KR protection is dependent upon security partners keeping their databases and data systems current. Over the long term, the level of cooperation and commitment needed for this must be sustained by a trusted working relationship between various security partners. This requires that information regarded as sensitive by providers be protected from unauthorized access, use, or disclosure; data content, accuracy, and currency, must also be protected from tampering or other corruption.
- **Durable Information:** The complexity, scope, and magnitude of the U.S. infrastructure require reliance on multiple sources that are acquired over long periods of time. As a result, information pertaining to the characteristics and quality of the data must be provided along with the actual data from each source. This requires the use of a common and standardized format, data scheme, and categorization system that is viable over the long term. DHS and SSAs are responsible for working together to establish and utilize the appropriate data collection formats. The DHS taxonomy is the foundation for multiple DHS programs that focus on CI/KR information such as the National Asset Database and the National Threat Incident Database. This taxonomy provides the foundation for a national-level information scheme.
- **Recurring Nature of Information Needs:** The process of information identification and additional data collection is a recurring need. Data requirements and availability are continually reassessed based on the current threat environment, analyses to identify gaps, or other factors. Focused data calls, in coordination with the SSAs and the States as appropriate, to specific sectors or locales may be required to fill identified information gaps. This imposes a continuing need for resources to constantly build and to update the system over the long term.

6.4.2 Simulation and Modeling

All security partners make use of simulations and modeling to comprehensively examine the potential consequences of terrorist exploitation of CI/KR, including an important focus on sector and cross-sector dependency and interdependency vulnerabilities. Continuous maintenance and update are required for these tools to produce reliable projections. Over the long term, new tools are needed to address fundamental changes due to factors such as technology, threats, or the business environment.

The DHS Preparedness Directorate will be the lead for modeling and simulation capabilities for CI/KR protection. In this capacity, the DHS Preparedness Directorate will:

- Coordinate with the DHS S&T Directorate on requirements for the development, maintenance, and use of research-related modeling capabilities for CI/KR protection;

- Specify requirements for the development, maintenance, and use of operations-related modeling capabilities for CI/KR protection in coordination with the DHS S&T Directorate and SSAs, as appropriate;
- Work with end-users to design operations-related tools that provide maximum utility and clarity for CI/KR protection activities in both emergencies and routine operations;
- Review existing private sector modeling initiatives and opportunities for joint ventures to ensure that DHS and its security partners make maximum use of private sector modeling capabilities;
- Coordinate with SSAs that have relevant modeling capabilities to develop appropriate mechanisms for the development, maintenance, and use of such for CI/KR protection as directed by HSPD-7; and
- Familiarize SSAs and other security partners with the availability of relevant modeling and simulation capabilities through training and exercises.

The National Infrastructure Simulation and Analysis Center (NISAC) provides advanced modeling and simulation capabilities for the analysis of CI/KR interdependencies, vulnerabilities, and other complex phenomena. In accordance with the Homeland Security Act, DHS provides the program office for NISAC and manages the development, maintenance, and use of relevant modeling capabilities by NISAC for CI/KR protection.

6.4.3 Coordination With Security Partners on Databases and Modeling

Integrating existing databases into DHS databases, such as the NADB, not only reduces duplication of effort, but also ensures that available data is consistent, current, and accurate, and provides users with a consolidated picture across all CI/KR sectors. However, this approach is effective only if the source information is maintained properly. Maintaining a current and useful database involves the support, coordination, and commitment of the SSAs, private sector entities, and other security partners. Because the most current and accurate CI/KR-related data is best known by owners and operators, the effectiveness of the effort depends on all security partners keeping their databases and data systems current. As the responsible agent for the identification of assets and existing databases for their sectors, the SSAs will:

- Outline in their SSPs the sector plans and processes for the database, data system, modeling and simulation, development, and updates;
- Work with sector security partners to facilitate the collection of accurate information for database, data system, and modeling and simulation use;
- Specify the timelines and milestones for the initial population of asset databases; and
- Specify a regular schedule for maintenance and updating of the databases.

DHS will work with SSAs and other security partners to:

- Identify databases and other data services that will be integrated with CI/KR protection databases and data systems;
- Facilitate the actual integration of databases or importation of data into CI/KR protection databases and data systems, using a common and standardized format, data scheme, and categorization system or taxonomy specified by DHS in coordination with the SSAs; and

- Define the schedule for importing databases into such systems as the NADB.

6.5 Continuously Improving the NIPP and the SSPs

The NIPP uses the Federal Senior Leadership Council and the Partnership for Critical Infrastructure Security as the primary forums for coordination of policy, planning, training, and other requirements needed to ensure efficient implementation and ongoing management and maintenance of the NIPP and SSPs.

6.5.1 Management and Coordination

DHS is the Federal executive agent for NIPP management and maintenance.

The NIPP is a multiyear plan describing mechanisms for sustaining the Nation's steady-state protective posture. The NIPP and its component SSPs include a process for annual review; periodic interim updates as required; and regularly scheduled full reviews and re-issuance every three years, or more frequently, if directed by the Secretary of Homeland Security.

DHS/OIP will oversee the review and maintenance process for the NIPP; SSAs, in coordination with the GCCs and SCCs, will establish and operate the mechanism(s) necessary to coordinate this effort for their respective SSPs. The NIPP and SSP revision processes will include developing or updating any documents necessary to carry out NIPP activities. The NIPP will be reviewed at least annually to:

- Measure accomplishments in support of program goals and objectives;
- Ensure that the Plan adequately reflects the level of resources available and budgeted;
- Adjust activities and initiatives based on national risk analysis;
- Incorporate lessons learned and best practices from exercises and actual incidents and alerts; and
- Reflect progress in the Nation's CIKR protection, as well as changes to national priorities, critical tasks, and capabilities outlined in the National Preparedness Goal.

As changes are warranted, periodic updates to the NIPP will be issued. Types of developments that merit a periodic update include new laws, executive orders, Presidential directives, or regulations, and procedural changes to NIPP activities based on real-world incidents or exercise experiences.

6.5.2 Maintenance and Updating

The following paragraphs establish the procedures for interim changes and full updating of the NIPP:

- **Types of Changes:** Changes include additions of new or supplementary material and deletions. No proposed change should contradict or override authorities or other plans contained in statute, executive order, or regulation.
- **Coordination and Approval:** While DHS is the Federal executive agent for NIPP management and maintenance, any Federal department or agency with assigned responsibilities under the NIPP may propose a change to the Plan. DHS is responsible for coordinating the review and approval of all proposed modifications to the NIPP with SSAs and other security partners, as appropriate.

- 1 • **Notice of Change:** DHS will issue an official Notice of Change for each interim revision to the NIPP.
2 After publication, the modifications will be considered part of the NIPP for operational purposes
3 pending a formal revision and re-issuance of the entire document. Interim changes can be further
4 modified or updated using this process.
 - 5 • **Distribution:** DHS will distribute Notices of Change to all participating security partners. Notices of
6 change to other organizations will be provided upon request.
 - 7 • **Re-Issuance:** DHS will coordinate full reviews and updating of the NIPP every three years, or more
8 frequently, if the Secretary deems necessary. The review and updating will consider lessons learned
9 and best practices identified during implementation in each sector and incorporate the periodic
10 changes and any new information technologies. DHS will distribute revised NIPP documents for
11 interagency review and concurrence.
- 12 SSAs, in coordination with the GCCs and SCCs, will establish and operate the mechanism(s) necessary to
13 coordinate ongoing SSP management and maintenance in accordance with the process established for the
14 NIPP.

7. Providing Resources for the CI/KR Protection Program

Investing in CI/KR protection activities requires an integrated, judicious process to ensure that our limited resources are applied to our most critical needs. Since the September 11, 2001, attacks, CI/KR protection expenditures have increased among security partners across all sectors and jurisdictional levels. With finite Federal resources available to support protection of the Nation's CI/KR, the NIPP serves as the unifying framework that is needed to ensure that CI/KR investments across the Nation are coordinated and reflect the highest priorities, based on risk and need, for achieving the homeland security mission.

This chapter describes an integrated risk-based approach that will be used to help determine how CI/KR protection programs at the Federal level will be funded through appropriations to DHS, the SSAs, and other Federal entities; how State- and local-level CI/KR protection efforts will be supported through DHS grant programs; and how all of these investments, coupled with appropriate incentives, support collaboration among security partners. Implementation of this coordinated budget and resource process will require collaboration and cooperation between DHS, the SSAs, and other security partners to establish priorities, define requirements, share information, and maximize the use of finite resources.

7.1 The Risk-Based Resource Allocation Process

Funding in support of CI/KR protection programs at all levels is guided by a straightforward principle: *Resources must be directed to areas of greatest priority in order to effectively manage risk.* By definition, all CI/KR assets, systems, and networks are important to the Nation. However, given the limitations of resources and considering the risk factors of threat, vulnerability, and consequence, some assets, systems, or networks are deemed to be more critical to the Nation as a whole than others. This chapter provides a process to ensure that we identify and prioritize resource requirements for our most critical CI/KR protection needs through an integrated approach that incorporates the input and perspective of DHS, the SSAs, State and local governments, and other security partners, while working with the Executive Office of the President (EOP) to determine national funding priorities.

This risk-based resource allocation process allows DHS to identify those assets, systems, and networks that are most critical from a national perspective, and supports a coordinated and cohesive nationwide CI/KR protection effort. Through this process, DHS works with the SSAs and State governments to aggregate information and build a comprehensive picture of infrastructure protection efforts across the Nation. This understanding informs resource allocation decisions by ensuring that resources are allocated to areas of greatest priority.

To build this comprehensive assessment of national CI/KR protection efforts, DHS must work with SSAs and State and local governments to gain an understanding of how CI/KR protection is being conducted across the country, what priorities and requirements drive these efforts, and how such efforts are funded. DHS can then use this information to identify those assets, systems, and networks whose protection is of the highest priority from a national perspective, and ensure that the appropriate programs or protection efforts are adequately funded. Likewise, DHS can also identify duplicative efforts and gaps in CI/KR protection across sectors and jurisdictions. DHS will work with the SSAs and State governments to collect this information.

7.1.1 Sector-Specific Agency Reporting to DHS

Given their unique individual risk landscapes, CI/KR sectors each face different infrastructure protection challenges. For instance, some sectors have distinct, easily identifiable assets that are easily prioritized. Others may have thousands of identical assets, all of which are equally critical. Others, still, are made up of systems or networks, as opposed to distinct assets, for which specific protective measures are not easily defined. Furthermore, interdependencies among sectors can cause duplicative protection efforts or lead to gaps in funding for CI/KR protection. To ensure that resources are allocated according to national priorities based on national risk and need, DHS must be able to accurately assess priorities, requirements, and efforts across these diverse sectors.

The SSAs, supported by their respective Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs), are best equipped to represent their sector's individual CI/KR protection efforts in this national assessment. Consistent with HSPD-7, each SSA is required to develop and submit to DHS an Annual Report that identifies existing CI/KR protection programs, NIPP-related initiatives, and relevant requirements for CI/KR protection for their sector. Therefore, the first step for SSAs in the risk-based resource allocation process is to accurately communicate their sector's priorities, requirements, and funding projections for CI/KR protection through this Annual Report. The SSAs will prepare the Annual Report with input from the SCCs and GCCs as appropriate. The Annual Report must be submitted to DHS by **July 1** of each year. The sector-specific information provided in this Annual Report that will inform resource allocation decisions includes:

- Priorities and annual goals for CI/KR protection;
- Sector-specific requirements for CI/KR protection activities and programs based on risk and need; and
- Projections for NIPP-related program funding that will be included in the SSA budget request to the Office of Management and Budget (OMB) as part of the annual Federal budget process.

7.1.2 State Government Reporting to DHS

Like sectors, State governments face diverse CI/KR protection challenges and have different priorities, requirements, and available resources. Furthermore, State CI/KR protection efforts are closely intertwined with those of other States, or with various sectors. To accurately assess the national CI/KR protection effort and to identify protection needs that warrant attention at a national level, DHS must aggregate information across States as it does across sectors.

The DHS Office of Grants and Training (G&T) requests that each State develop a homeland security strategy that establishes goals and objectives for its homeland security program and includes CI/KR protection as a core element. It also asks each State to develop a Program and Capability Enhancement Plan that prioritizes statewide resource needs to support this program. The States will work with DHS/G&T to use these mechanisms to establish their:

- Priorities and annual goals for CI/KR protection;
- State-specific requirements for CI/KR protection activities and programs, based on risk and need; and

- Projections for funding from DHS grants, described in further detail below, and other funding sources required to implement the NIPP and address their identified priorities and annual goals.

This information must be reported to DHS by the date specified in the grant guidance issued each year by DHS/G&T if it is to be considered in the CI/KR deliberations for the current Federal budget cycle.

7.1.3 Aggregating Submissions to DHS

DHS will use the information collected from the SSA and State Annual Reports to assess CI/KR protection efforts across the country and, from this assessment, identify national priorities and requirements based on national risk and need. DHS will collaborate with the Homeland Security Council (HSC) as it develops national-level priorities and requirements. Once national priorities and requirements have been identified based on this aggregated information, DHS will develop funding recommendations for programs and initiatives designed to reduce national-level risk in the CI/KR protection mission area. In cases where gaps or duplicative efforts exist, DHS will work with the SSAs and the States to rationalize individual requirements and recommend funding for national CI/KR protection priorities.

Once information from the sectors and States has been collected, national priorities and requirements have been determined, and funding projections have been evaluated, DHS will summarize this information in the National NIPP Funding Report. This Funding Report provides a comprehensive summary of national infrastructure protection priorities and requirements and, based on these, makes prioritized recommendations for resource allocation to meet national requirements. This Funding Report will be submitted to OMB on **September 1** as part of the annual Federal budget process.

This risk-based resource allocation process allows those responsible for infrastructure protection at all levels of government to direct resources to areas of greatest reduction in risk, while providing the Federal government with a method of ensuring that the Nation's most critical assets, systems, and networks receive priority resource focus. The information collected through this process will inform risk-based resource allocation decisions for both the SSAs and the States by actuating the allocation of Federal resources through two principal funding streams: Federal department and agency budgets and the homeland security grant programs.

7.2 Federal Resource Allocation Process for DHS, SSAs, and Other Federal Agencies

The Federal resource allocation process described in this section is designed to ensure that the collective efforts of DHS, the SSAs, and other Federal departments and agencies are consistent with the NIPP, national CI/KR protection strategy, and national priorities. It is also designed to be consistent with the DHS responsibility to coordinate overall national CI/KR protection and to identify national-level gaps, overlaps, or shortfalls in protecting CI/KR. Driven in large part by existing and well-understood Federal budget milestones, the process is integrated with existing OMB budget processes and requirements. The specific roles of DHS, the SSAs, and the EOP are described in further detail below.

7.2.1 Department of Homeland Security

DHS is responsible for overall coordination of the Nation's CI/KR protection efforts. To carry out this responsibility, DHS must identify and prioritize nationally critical assets, systems, and networks; ensure that appropriate protective initiatives exist or are implemented; and address any gaps or shortfalls in the protection of nationally critical CI/KR. DHS works closely with the EOP (e.g., HSC, OMB) to aggregate NIPP-related activities and related budget requests from the SSAs and other Federal departments and agencies to ensure a uniform decision-making process that makes informed judgments and tradeoffs in prioritizing Federal investments.

At the beginning of the budget process, DHS works with the HSC to establish a national CI/KR protection strategic approach and priorities, and with the SSAs to develop sector-specific NIPP-related requirements. Driven largely by the identification and prioritization of critical assets, systems, and networks across sectors and States, this will help inform resource allocation decisions later in the process. The SSAs communicate their existing NIPP-related programs to DHS through their Annual Reports. DHS uses the Annual Reports to conduct an assessment of the comprehensive picture of national NIPP-related investment. Additionally, DHS, the SSAs, and other Federal departments and agencies must identify all NIPP-related programs and initiatives as part of their annual departmental budget request submitted to OMB. DHS will then submit to the EOP, the National NIPP Funding Report, which is a summary report of national NIPP-related investment recommendations. In this Funding Report, DHS will identify the NIPP requirements and summarize NIPP funding requests across sectors. This Funding Report will provide OMB with a comprehensive picture, allowing for the identification of areas where the NIPP requirements are not met and where additional risk-based funding is needed.

7.2.2 Sector-Specific Agencies

Earlier chapters of the NIPP articulate how DHS and the SSAs will work with the respective CI/KR sectors to determine risks and set priorities. Based on guidance from DHS, each SSA will develop and maintain current an SSP that supports the overarching NIPP goals and objectives. Additionally, the SSAs are responsible for determining sector-specific priorities and requirements. These priorities and requirements will be submitted to DHS in their Annual Reports along with funding projections. The SSAs will work within their respective department or agency budget process to develop the NIPP-related aspects of their budget submissions that are designed to meet national NIPP requirements. The SSAs will also work within their respective departments or agencies to coordinate with OMB and DHS during the subsequent deliberations, such as the budget passback, to ensure that any gaps or shortcomings in NIPP-related funding are addressed.

Additionally, the subset of CI/KR protection funding requirements directed toward R&D and Science and Technology (S&T) investment will be highlighted by the SSAs, SCCs, and GCCs in the Annual Reports to inform the NCIP R&D Plan and its technology roadmap, while ensuring efficient coordination with the DHS R&D/S&T community and supporting the Federal research and technology base. These R&D and S&T plans and requirements will be based on the R&D planning section of each sector's SSP. The identified R&D requirements will be prioritized based on the potential increase in CI/KR protection capabilities for a given investment.

7.2.3 Executive Office of the President

The EOP works with DHS to establish national NIPP priorities and maintain an ongoing dialog regarding CI/KR protection requirements, priorities, and resources throughout the year. Upon submission of the DHS National NIPP Funding Report, the EOP will work with DHS to identify gaps between proposed CI/KR protection funding and the national NIPP requirements based on department and agency budget submissions. The EOP reviews the Funding Report to address any outstanding policy or budgetary issues requiring interagency coordination and approval. Ultimately, the EOP will act as the final policy arbiter for funding decisions related to Federal CI/KR protection programs.

7.2.4 Summary of Roles and Responsibilities

Figure 7-1 outlines the roles and responsibilities of DHS, the SSAs, and the EOP throughout this process, as well as the timelines associated with major activities.

	DHS	Sector Specific Agencies	Executive Office of the President
Feb-July	<ul style="list-style-type: none"> Work with HSC to establish national NIPP priorities Through partnership mechanisms such as SCC and GCC, work with SSAs to develop national and sector-specific NIPP requirements 	<ul style="list-style-type: none"> Work with DHS in development of national and sector-specific NIPP requirements Develop NIPP-related aspect of budget submission with support of DHS where necessary and consistent with NIPP requirements established through collaborative process 	<ul style="list-style-type: none"> Work with DHS in establishing national NIPP priorities
July-Sep	<ul style="list-style-type: none"> Aggregate Annual Reports from all sectors to develop picture of national NIPP-related investment Submit budget request to OMB on Sep 1 Submit summary report on Sep 1 of national NIPP-related investments and requirements 	<ul style="list-style-type: none"> On July 1, submit Annual Report to DHS that includes summary of existing NIPP-related programs On Sep 1, submit budget request to OMB 	<ul style="list-style-type: none"> Maintain ongoing dialogue with DHS concerning national NIPP priorities
Sep-Feb	<ul style="list-style-type: none"> Work with OMB and SSAs during budget passback to remedy any gaps or shortcomings in NIPP-related funding, focusing on ensuring funding of programs associated with nationally critical assets or systems 	<ul style="list-style-type: none"> Work with OMB and DHS during budget passback to remedy any gaps or shortcomings in NIPP-related funding 	<ul style="list-style-type: none"> Assess DHS summary report of NIPP-related investment against national NIPP priorities—identify gaps Work with DHS and SSAs during budget passback to remedy funding gaps Submit budget first Monday in February

Figure 7-1: DHS, SSA, and EOP Roles and Responsibilities in Federal Resource Allocation

The final determination of funding priorities, based on the collaborative efforts of DHS, the SSAs, and other Federal departments and agencies with the EOP, will guide CI/KR protection programs and the allocation of resources in support of the NIPP. These priorities will not only support Federal government (DHS and SSA) infrastructure protection activities, but they also will guide and support homeland security and CI/KR protection activities across and within State, local, and tribal jurisdictions. Federal funding, as authorized and appropriated by Congress, provides the basis for the allocation of grants available to support the homeland security and infrastructure protection efforts of State, local, and tribal jurisdictions. These funds will be allocated to State, local, and tribal jurisdictions, based on guidance from appropriations laws, program guidance requirements, and national priorities, as identified by DHS, the SSAs, other Federal departments and agencies, and the EOP.

7.3 Federal Resources for State and Local Government Preparedness

Federal grants from DHS and other departments, and other resources such as training and technical assistance, offer key support to State and local jurisdictions for nationwide CI/KR protection programs. These grants and other programs provide avenues for directing Federal resources to meet the CI/KR needs that are more appropriately managed by State and local entities.

DHS/G&T is responsible for coordinating Federal homeland security grant programs to help State, local, and tribal governments enhance their ability to prevent, protect against, respond to, and recover from terrorist acts or threats and other hazards. DHS/G&T offers State, local, and tribal security partners access to significant funding through several grant programs that can be leveraged to support CI/KR protection requirements based on risk and need.

Federal grants available through DHS/G&T can be grouped into two broad categories: (1) *overarching homeland security grant programs* that provide funding for a broad set of activities in support of homeland security mission areas and the national priorities outlined in the National Preparedness Goal, and (2) *targeted infrastructure protection programs* for specific CI/KR-related protection initiatives and programs within identified jurisdictions. This allows the different jurisdictions to leverage the range of available resources, including those from Federal, State, local, and tribal sources, as appropriate, in support of the protection activities needed to reduce risk and close the identified capability gaps related to CI/KR protection within their jurisdictions.

Overarching Homeland Security Grant Programs

The overarching Homeland Security Grant Program supports activities that are conducted in accordance with the National Preparedness Goal. These funds support overall State, local, and tribal homeland security efforts, and can be leveraged to support State, regional, local, and/or tribal CI/KR protection programs. These funds are allocated in coordination with national CI/KR protection efforts.

The primary overarching homeland security grant programs include:

- **Law Enforcement Terrorism Prevention Program (LETPP):** The LETPP focuses on the prevention of, and protection against, terrorist attacks, and provides law enforcement and public safety communities with funds to support the following activities: intelligence gathering and information sharing through the enhancement/establishment of fusion centers; hardening of high-value targets; strategic planning; building interoperable communications; and collaboration with non-law-enforcement partners, other government agencies, and the private sector.
- **State Homeland Security Program (SHSP):** The SHSP supports the implementation of the State Homeland Security Strategy to address identified planning, equipment, training, and exercise needs. In addition, SHSP supports the implementation of the National Preparedness Goal, the National Incident Management System (NIMS), the NRP, and the NIPP to support the prevention of, protection against, response to, and recovery from acts of terrorism.
- **Targeted Infrastructure Protection Programs:** These Programs include grants for specific activities that focus on the protection of CI/KR, such as ports, mass transit, rail transportation, etc. These funds

support CI/KR protection capabilities based on risk and need in coordination with DHS, SSA, and Federal priorities.

- **Urban Areas Security Initiative (UASI):** UASI funds address the unique planning, equipment, training, and exercise needs of high-threat, high-density Urban Areas, and assist them in building an enhanced and sustainable capacity to prevent, protect against, respond to, and recover from acts of terrorism.

The primary targeted infrastructure protection grant programs include:

- **Buffer Zone Protection Program (BZPP) (managed in conjunction with the DHS/OIP):** The BZPP provides funding for enhanced security of CI/KR. This program establishes Buffer Zone Plans that are intended to assist local law enforcement and emergency responders develop and implement protective and preventive measures around high-priority infrastructure targets.
- **Intercity Bus Security Grant Program (IBSGP):** The IBSGP provides financial assistance to owners and operators of fixed-route, intercity bus services, and special-needs charter buses to improve security for operators and passengers. The program strives to create a sustainable effort for the protection of CI/KR from terrorism or any other incidents that would cause major loss of life and severe disruption.
- **Intercity Passenger Rail Security Grant Program (IPRSGP):** The IPRSGP provides financial assistance to Amtrak for the protection of CI/KR and preparedness activities related to acts of terrorism or other incidents.
- **Port Security Grant Program (PSGP):** The PSGP funds owners and operators of ports, terminals, and U.S.-inspected passenger vessels and ferries, as well as port authorities and State and local agencies, to improve security for operators and passengers through physical security enhancements. The program strives to create a sustainable, risk-based effort for the protection of CI/KR from terrorism or any other incidents that would cause major loss of life and severe disruption to commerce.
- **Transit Security Grant Program (TSGP):** The TSGP provides funding to support security enhancements for intra-city passenger rail transportation and other security measures. The program addresses prevention and protection activities for three transit modalities: rail transit, intra-city bus transit, and ferry systems.

DHS/OIP and DHS/G&T will focus targeted infrastructure protection grant programs, such as the BZPP and transportation security grants, to support national-level CI/KR protection priorities and to **reinforce** activities funded through Federal department and agency budgets and other homeland security grant programs. States and localities are responsible for ensuring the identification and implementation of protection initiatives for CI/KR that are deemed to be critical within the jurisdiction. Grantees should apply the resources available under the overarching homeland security grant programs, such as SHSP, UASI, and LETPP, to address their regionally or locally critical priority CI/KR protection initiatives. A combination of grant program funding may be necessary to enable the protection of assets, systems, or networks deemed to be nationally critical. The protection of national-level CI/KR will be the top priority of all Federally funded initiatives and programs.

Available DHS/G&T grant funding is awarded to the Governor-appointed State Administrative Agency (SAA), which serves in each State as the lead for homeland security program implementation. Through their respective SAAs, States will identify and prioritize their homeland security needs – including CI/KR

protection – and leverage assistance from these funding streams according to the priorities identified in their State Homeland Security Strategies, and Program and Capability Enhancement Plans. These planning processes, undertaken at the State level, are built on the common framework articulated in the National Preparedness Goal, the National Priorities – including implementation of the NIPP – and the Target Capabilities List.

DHS will provide State, local, and tribal authorities with additional guidance on how to identify, assess, and prioritize CI/KR protection needs and programs in support of the National Preparedness Goal as they apply for homeland security grants. Additional information on DHS grant programs, guidelines, allocations, and eligibility is available at <http://www.ojp.usdoj.gov/odp>.

7.4 Setting an Agenda in Collaboration With CI/KR Protection Security Partners

Government resource allocation decisions for CI/KR protection at all levels of government should align as integral components of the unified, national approach established in the NIPP. In accordance with the responsibilities established in HSPD-7, DHS works with the SSAs and other security partners to set the national agenda that specifies this strategic approach to CI/KR protection, articulates the requirements associated with that agenda, and supports collaboration among security partners. While the Federal government's funding of programs and initiatives that support CI/KR protection makes a significant contribution to the security of the Nation, a fully successful effort requires DHS; the SSAs; and State, local, and tribal governments to work closely with the private sector to promote the most efficient voluntary use of resources by asset owners and operators.

The NIPP uses the risk management framework to support coordination between security partners outside the Federal government. Each step of the risk management framework presents opportunities for collaboration between and among all security partners. Coordination between State and local agencies and the sectors themselves ensures that cross-sector needs and priorities are accurately identified and understood. Government coordination with private sector owners and operators is required throughout the process to ensure a unified national CI/KR protection effort, provide accurate identification of CI/KR assets and systems, provide risk-related information, ensure implementation of appropriate protective measures, measure program effectiveness, and make improvements.

These opportunities for collaboration allow private sector owners and operators to benefit from CI/KR protection investments in a number of ways. First, investments in CI/KR protection will help protect infrastructure from all hazards, including common threats posed by malicious individuals or acts of nature, in addition to those posed by terrorist organizations. Second, continuity-of-business planning can facilitate recovery of commercial activity after an incident. Finally, investing in CI/KR protection within the NIPP framework will help private sector owners and operators enhance protective measures, and it will support their decision makers with more comprehensive threat and vulnerability information. DHS explores new opportunities to encourage such collaboration through incentives, regulatory changes, and providing more useful information on risk assessment and management.

1 List of Acronyms and Abbreviations

2	ANSI	American National Standards Institute
3	APCERT	Asia Pacific Computer Emergency Response Team
4	APEC	Asia Pacific Economic Cooperation
5	BZPP	Buffer Zone Protection Program
6	CAEIAE	Centers of Academic Excellence in Information Assurance Education
7	CFIUS	Committee on Foreign Investment in the United States
8	CII	Critical Infrastructure Information
9	CI/KR	Critical Infrastructure/Key Resources
10	COI	Communities of Interest
11	COP	Common Operational Picture
12	CSIA IWG	Cybersecurity and Information Assurance Interagency Working Group
13	CSIRT	Computer Security Incident Response Teams
14	CWIN	Critical Infrastructure Warning Information Network
15	DHS	Department of Homeland Security
16	ECTF	Electronic Crime Task Force
17	EOC	Emergency Operations Center
18	EOP	Executive Office of the President
19	EPA	Environmental Protection Agency
20	FBI	Federal Bureau of Investigation
21	FOIA	Freedom of Information Act
22	FPS	Federal Protective Service
23	G&T	Grants and Training
24	GCC	Government Coordinating Council
25	HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
26	HSA	Homeland Security Advisor
27	HSAs	Homeland Security Advisors
28	HSAC	Homeland Security Advisory Council
29	HSAS	Homeland Security Advisory System
30	HSC	Homeland Security Council
31	HSDN	Homeland Security Data Network
32	HSIN	Homeland Security Information Network
33	HSIN-CS	HSIN-Critical Sector
34	HSIN-CT	HSIN-Counter Terrorism
35	HSIN-EM	HSIN-Emergency Management
36	HSIN-LE	HSIN-Law Enforcement
37	HSOC	Homeland Security Operations Center
38	HSPD	Homeland Security Presidential Directive
39	HSSP	Homeland Security Standards Panel
40	IBSGP	Intercity Bus Security Grant Program
41	IC	Intelligence Community
42	IIMG	Interagency Incident Management Group
43	IP	Infrastructure Protection (Division of DHS Preparedness Directorate)
44	IPRSGP	Intercity Passenger Rail Security Grant Program

1	ISAC	Information Sharing and Analysis Center
2	IT	Information Technology
3	JRIES	Joint Regional Information Exchange System
4	LE-A	Law Enforcement-Analysis
5	LEO	Law Enforcement Online
6	LETPP	Law Enforcement Terrorism Prevention Program
7	MBA	Master of Business Administration
8	NADB	National Asset Database
9	NAS	National Airspace System
10	NATO	North Atlantic Treaty Organization
11	NCC	National Coordinating Center [for Telecommunications]
12	NCIP R&D	National Critical Infrastructure Protection Research and Development
13	NCR	National Capital Region
14	NIAC	National Infrastructure Advisory Council
15	NICC	National Infrastructure Coordinating Center
16	NIMS	National Incident Management System
17	NIPP	National Infrastructure Protection Plan
18	NISAC	National Infrastructure Simulation and Analysis Center
19	NIST	National Institute of Standards and Technology
20	NITRD	Networking and Information Technology Research and Development
21	NRP	National Response Plan
22	NSA	National Security Agency
23	NS/EP	National Security/Emergency Preparedness
24	NSSE	National Special Security Event
25	NSTAC	National Security Telecommunications Advisory Committee
26	NSTC	National Science and Technology Council
27	OAS	Organization of American States
28	OECD	Organization for Economic Cooperation and Development
29	OI&A	Office of Intelligence and Analysis
30	OIP	Office of Infrastructure Protection (Division of DHS Preparedness Directorate)
31	OMB	Office of Management and Budget
32	OSTP	Office of Science and Technology Policy
33	P3	Public, Private, Partnership
34	PCII	Protected Critical Infrastructure Information
35	PCIS	Partnership for Critical Infrastructure Security
36	PDD	Presidential Decision Directive
37	PITAC	President's Information Technology Advisory Committee
38	PSA	Protective Security Advisor
39	PSGP	Port Security Grant Program
40	PVTSAC	Private Sector Senior Advisory Committee
41	RAMCAP	Risk Analysis and Management for Critical Asset Protection
42	R&D	Research and Development
43	SAA	State Administrative Agency
44	SAVs	Site Assistance Visits
45	SCADA	Supervisory Control and Data Acquisition
46	SCC	Sector Coordinating Council
47	SCEPC	Senior Civil Emergency Planning Committee

1	SFS	Scholarship for Service
2	SHSP	State Homeland Security Program
3	SPP	Security and Prosperity Partnership of North America
4	SSA	Sector-Specific Agency
5	SSI	Sensitive Security Information
6	SSP	Sector-Specific Plan
7	S&T	Science and Technology Directorate of DHS
8	SVA	Security Vulnerability Assessment
9	TCL	Target Capabilities List
10	TSA	Transportation Security Administration
11	TSGP	Transit Security Grant Program
12	UASI	Urban Areas Security Initiative
13	UCNI	Unclassified Controlled Nuclear Information
14	U.S.	United States
15	US-CERT	United States Computer Emergency Readiness Team
16	USCG	United States Coast Guard
17	UTL	Universal Task List
18		

- 1 Appendix 1: Special Considerations
- 2 Appendix 1A: Cross-Sector Cybersecurity
- 3 Appendix 1B: International CI/KR Protection

Appendix 1A: Cross-Sector Cybersecurity

This appendix provides additional details on the processes, procedures, and mechanisms needed to achieve NIPP goals and supporting objectives regarding cybersecurity. It specifies cybersecurity roles and responsibilities, coordination, processes, initiatives to reduce risk, and milestones and metrics to measure progress.

This appendix provides information concerning the *users* of cyber infrastructure, including CI/KR sectors and their associated security partners. Matters concerning *producers* of cyber infrastructure (i.e., the information technology (IT) industrial base) are addressed in the IT SSP. This appendix is organized to align with the corresponding chapters of the NIPP to provide the reader with the context for the additional information as follows:

1A.1 Introduction

1A.2 Responsibilities

1A.3 Managing Cyber Risk

1A.4 Ensuring Long-Term Cybersecurity

1A.1 Introduction

The U.S. economy and national security are highly dependent upon cyber infrastructure. Cyber infrastructure enables the Nation's essential services, resulting in a highly interconnected and interdependent network of CI/KR. This network enables services such as the Internet and financial markets, and also assists in the control of many critical processes, including the electric power grid and chemical processing plants, among various others.

A spectrum of malicious actors can and do conduct attacks against critical cyber infrastructure on an ongoing basis. Of primary concern is the risk of organized cyber attacks capable of causing debilitating disruption to the Nation's CI/KR, economy, or national security. Furthermore, while terrorist groups have not yet initiated a major attack against the Internet, there is ample evidence of their using it as a means of attack or for other purposes that support terrorist activities.

CI/KR functions and services are enabled through IT systems and services; however, if cybersecurity is not appropriately provided for, the risk to CI/KR is greatly increased.

DHS is committed to securing cyberspace by working collaboratively with public, private, academic, and international entities to enhance awareness and preparedness, as well as to ensure that the cyber elements of the critical infrastructure are:

- Robust and resilient enough to withstand attacks without incurring catastrophic damage;
- Responsive enough to recover from attacks in a timely manner; and
- Resilient enough to sustain nationally critical operations.

1A.1.1 Definitions

The following definitions explain key terms and concepts related to the cyber dimension of CI/KR protection:

- **Cyber infrastructure:** Includes electronic information and communications systems and the information contained in those systems. Information and communications systems are composed of all hardware and software that process (i.e., create, access, modify, and destroy), store (e.g., all media types: paper, magnetic, and electronic), and communicate (i.e., share and distribute) information, or any combination of all of these elements. For example, computer systems, control systems (e.g., Supervisory Control and Data Acquisition (SCADA) systems), and networks, such as the Internet, are part of cyber infrastructure:
 - *Producers* of cyber infrastructure are the IT industrial base, which comprise the IT Sector. The producers of cyber infrastructure play a key role in developing secure and reliable products.
 - *Consumers* of cyber infrastructure must maintain its security in a changing threat environment. Individuals, whether private citizens or employees with cyber systems administration responsibility, play a significant role in managing the security of computer systems to ensure that they are not used to enable attacks against CI/KR.
- **Cybersecurity:** The prevention of damage to, unauthorized use of, exploitation of, and, if needed, the restoration of electronic information and communications systems (and the information contained therein) to ensure confidentiality, integrity, and availability.
- **Cross-Sector Cybersecurity:** Collaborative efforts between DHS, the SSAs, and other security partners to secure cyber elements in an appropriate and consistent manner across sectors.

1A.1.2 Cyber-Specific Authorities

Various Federal strategies, directives, policies, and regulations provide the basis for Federal actions and activities associated with implementing the cyber-specific aspects of the NIPP. The two primary authorities associated with cybersecurity are the National Strategy to Secure Cyberspace and HSPD-7. These documents are described in further detail in Chapters 2 and 5 of the NIPP.

1A.2 Cybersecurity Responsibilities

The National Strategy to Secure Cyberspace and HSPD-7 identify the responsibilities of the various security partners with a role in securing cyberspace. These roles and responsibilities are described in more detail below.

1A.2.1 Department of Homeland Security

In accordance with Paragraph 16 of HSPD-7, DHS is a principal focal point for the security of cyberspace. DHS has specific responsibilities regarding the coordination of the efforts of security partners to prevent damage to, and unauthorized use and exploitation of, and enable the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. These responsibilities include:

- Developing a comprehensive national plan for securing U.S. CI/KR;
- Providing crisis management in response to attacks on critical information systems;
- Providing technical assistance to the private sector and other government entities with respect to emergency recovery plans for failures of critical information systems;
- Coordinating with other agencies of the Federal government to provide specific warning information and advice on appropriate protective measures and countermeasures to State, local, tribal, and non-governmental organizations, including the private sector, academia, and the public;
- Conducting and funding cybersecurity R&D, in partnership with other agencies, that will lead to new scientific understanding and technologies in support of homeland security; and
- Assisting SSAs in understanding and mitigating cyber risk and in developing effective and appropriate protective measures.

Within the risk management framework described in the NIPP, DHS is also responsible for the following activities:

- Providing cyber-specific expertise and assistance in addressing the cyber elements of CI/KR;
- Promoting a comprehensive national awareness program to empower businesses, the workforce, and individuals to secure their own segments of cyberspace;
- Working with security partners to reduce cyber vulnerabilities and minimize the severity of cyber attacks;
- Leading the development and conduct of a national cyber threat assessment;
- Facilitating cross-sector cyber analysis to understand and mitigate cyber risk;
- Providing guidance, review, and functional advice on the development of effective and appropriate cyber-protective measures; and
- Coordinating cybersecurity protective programs and contingency plans, including a plan for recovering Internet functions.

1A.2.2 Sector-Specific Agencies

Recognizing that each CI/KR sector possesses its own unique characteristics and operating models, SSAs provide the subject matter and industry expertise through relationships with the private sector to ensure protection of the assets, systems, and networks within their sectors. SSAs must understand and mitigate cyber risk by:

- Identifying subject matter expertise pertinent to the cyber aspects of their sector;
- Increasing awareness of how the business and operational aspects of the sector rely on cyber systems and processes;

- Determining whether approaches for asset identification, risk assessment, and protective measures currently address cyber assets, systems, and networks; require enhancement; or require use of alternative approaches;
- Reviewing and modifying existing and future sector efforts to ensure that cyber concerns are fully integrated into sector security strategies and protective activities;
- Establishing mutual assistance programs for cybersecurity emergencies; and
- Exchanging cyber-specific information with sector security partners, including the international community, as appropriate, to improve the Nation's overall cybersecurity posture.

1A.2.3 Other Federal Departments and Agencies

All Federal departments and agencies must manage the security of their computer systems while maintaining awareness of vulnerabilities and consequences to ensure that computer systems are not used to enable attacks against the Nation's CI/KR. A number of Federal agencies have specific additional responsibilities outlined in the National Strategy to Secure Cyberspace:

- **The Department of Justice and the Federal Trade Commission:** Working with sectors to address barriers to mutual assistance programs for cybersecurity emergencies.
- **The Department of Justice and Other Federal Agencies:**
 - Developing and implementing efforts to reduce cyber attacks and cyber threats by developing more robust data on victims of cyber crime and intrusions;
 - Exploring means to provide sufficient investigative and forensic resources and training to facilitate expeditious investigation and resolution of CI/KR incidents; and
 - Identifying ways to improve cyber information sharing and investigative coordination within the Federal, State, local, and tribal law enforcement communities; other agencies; and the private sector.
- **The Federal Bureau of Investigation and Intelligence Community:** Ensuring a strong counterintelligence posture to counter cyber-based intelligence collection against the U.S. government, as well as commercial and educational organizations.
- **The Intelligence Community, the Department of Defense, and Law Enforcement Agencies:** Improving the Nation's ability to quickly attribute the source of threatening attacks or actions to enable timely and effective response.

1A.2.4 State, Local, and Tribal Governments

State, local, and tribal governments are encouraged to implement the following cyber recommendations:

- Managing the security of their computer systems while maintaining awareness of threats, vulnerabilities, and consequences to ensure that they are not used to enable attacks against CK/KR, and ensuring that all State government offices manage their computer systems accordingly;

- Participating in significant national, regional, and local awareness programs to encourage local governments and citizens to manage their computer systems appropriately; and
- Establishing cybersecurity programs, including awareness, audits, and standards.

1A.2.5 Private Sector

- The private sector is encouraged to implement the following recommendations as indicated in the National Strategy to Secure Cyberspace;
- Managing the security of their computer systems while maintaining awareness of vulnerabilities and consequences to ensure that computer systems are not used to enable attacks against the Nation's CI/KR;
- Reviewing and exercising IT continuity plans and considering diversity in IT service providers as a way of mitigating risk;
- Considering active involvement in sector-wide programs to share information on cybersecurity;
- Evaluating the security of networks that affect the security of the Nation's CI/KR, including:
 - Conducting audits to ensure effectiveness and use of best practices;
 - Developing continuity plans that consider off-site staff and equipment; and
 - Participating in industry-wide information sharing and best practices dissemination;
- Considering including in near-term R&D priorities, programs for highly secure and trustworthy operating systems; and
- Promoting more secure "out of the box" installation and implementation of software industry products, including increasing user awareness of the security features in products; ease of use for security functions; and, where feasible, promotion of industry guidelines and best practices that support such efforts.

1A.2.6 Academia

Colleges and universities are encouraged to implement several recommendations as indicated in the National Strategy to Secure Cyberspace:

- Managing the security of their computer systems while maintaining awareness of vulnerabilities and consequences to ensure that computer systems are not used to enable attacks against the Nation's CI/KR;
- Establishing appropriate information-sharing mechanisms to deal with cyber attacks and vulnerabilities;
- Establishing an on-call point of contact for Internet service providers and law enforcement officials in the event that the institution's cyber assets, systems, or networks are discovered to be launching cyber attacks; and
- Establishing model guidelines empowering Chief Information Officers to manage cybersecurity, develop and exchange best practices for cybersecurity, and promote model user awareness programs.

1A.3 Managing Cyber Risk

Under the NIPP, risk management follows a logical process that is comprised of the following fundamental activities: (1) setting security goals; (2) identifying assets, including cyber assets, systems, and networks; (3) assessing risk, which is based on consequences, threats, and vulnerability; (4) prioritizing efforts that will make the greatest reduction in risk; (5) implementing programs; and (6) measuring effectiveness and improving programs. Each of these is discussed as they pertain to the cyber dimension of CI/KR protection in the subsections that follow.

1A.3.1 Set Security Goals

The goals and objectives set forth in the NIPP provide the overarching direction for CI/KR protection. Five cybersecurity objectives support the NIPP:

Objective 1: Establish a National Cyberspace Security Response System

Establishing a National Cyberspace Security Response System will provide the following benefits, which will improve our ability to prevent, detect, respond to, and reconstitute rapidly after a cyber incident:

- Enhance information dissemination, awareness, and analysis of threats and responses, as well as improve situational awareness capabilities;
- Promote collaboration, coordination, and information sharing among public, private, and international communities;
- Promote an international cyber strategy to secure cyberspace;
- Protect government cyberspace; and
- Improve the Nation's cybersecurity readiness, protection, and incident response capabilities by creating, sponsoring, and learning from national, regional, and interagency exercises and workshops.

Section 3A.3.5 of this appendix describes government cybersecurity initiatives and programs, as well as exercise programs that promote effective collaborative response to cyber attack. Section 3A.4.1 of this appendix describes information sharing and international efforts to improve collaboration and coordination.

Objective 2: Reduce Vulnerabilities and Minimize the Severity of Cyber Attacks

Working with the public and private sectors to reduce vulnerabilities and minimize the severity of cyber attacks will help improve the cybersecurity of CI/KR by reducing risks to control systems and improving the security of software throughout its life cycle.

Objective 3: Promote a National Awareness Program

An important objective is to promote a comprehensive national awareness program to empower businesses, the workforce, and individuals to secure their own segments of cyberspace. This will help cyber CI/KR protection efforts by:

- Building and maintaining the trusted relationships between industry, government, and academia needed to raise cybersecurity awareness and foster collaborative efforts to secure cyberspace; and
- Enabling the dissemination of important information to key constituencies and foster collaboration with public, private, and international partners.

Section 3A.4.1 of this appendix describes outreach and awareness initiatives to empower security partners at all levels of government and the private sector to secure cyberspace.

Objective 4: Foster Cyber Training and Education Programs

Training and education are important components of establishing a knowledge base for the security of cyberspace. To attain the objective of fostering adequate training and education programs to support the Nation's cybersecurity needs, a cadre of cybersecurity professionals must be developed and maintained through training and education programs. Section 3A.4.3 of this appendix describes training and education programs to help develop cybersecurity professionals.

Objective 5: Identify and Reduce Threats to Cyberspace

Because of the nature of cyberspace, threats can emerge from anywhere at any time. Unlike physically based threats, cyber threats can be more difficult to identify and track. DHS, in collaboration with other security partners, will identify and reduce threats to cyberspace by:

- Improving a coordinated cyber intelligence capability; and
- Improving threat detection and deterrence capabilities.

Section 3A.4.1 of this appendix describes efforts to reduce cyber risk through improved interagency coordination.

1A.3.2 Identify Cyber Assets

During NIPP risk analysis, cyber assets, systems, and networks are examined both as individual entities and as one of the three basic elements (physical, cyber, and human) of a larger CI/KR asset, system, or network that must be identified as the starting point for risk analysis.

Cyber assets, systems, and networks represent a variety of hardware and software components that perform a particular function. Examples include networking equipment, database servers, security systems, operating systems, and database software. The following are examples of cyber assets, systems, or networks that exist in most, if not all, sectors and should be identified individually or included as a cyber element of a physical asset's description if they are associated with one:

- **Automated access control** is a process that is common to all sectors supporting physical access control, which includes embedded physical, cyber, and human elements. The physical and human elements are more commonly recognized, such as people possessing access cards and scanners outside of the facility. However, the cyber elements are less easily recognized because they are typically behind the scenes. These include the hardware and software that process, store, and

1 communicate electronic information, such as database servers that store individuals' names and
2 software that processes access attempts.

- 3 • **Control systems** are computer-based systems used within many infrastructures and industries to
4 monitor and control sensitive processes and physical functions. Control systems typically collect
5 measurement and operational data from the field, process and display the information, and relay
6 control commands to local or remote equipment or human-machine interfaces (operators). Various
7 types of control systems are used at the sector level in different ways. Examples include management
8 of the electric power grid using Supervisory Control and Data Acquisition (SCADA) systems within the
9 energy sector and process control systems that control the timing and volume of chemical processes
10 within the chemical sector. Control systems generally consist of two parts: (1) operator interfaces (also
11 known as human-machine interfaces), and (2) field controllers. Both are computer-based. These
12 systems are particularly problematic because their life cycle is typically 15+ years, in contrast to the 12-
13 to 18-month life cycle of many common business cyber systems. Typical cybersecurity measures do
14 not often work in this operations-oriented environment. Such control systems were designed for
15 specific uses in isolation, but are becoming connected to the business networks and are, thus,
16 vulnerable to various potential attack vectors.

17 The Internet has been identified as a key resource comprised of domestic and international assets within
18 both the IT and Telecommunications Sectors and is used by all sectors to varying degrees. While the
19 availability of the service is the responsibility of both the IT and Telecommunications Sectors, the need for
20 access to and reliance on the Internet are common to all sectors.

21 DHS, in collaboration with other security partners, provides a cross-sector cyber asset identification
22 methodology that, when applied, enables a sector to identify cyber entities and characterize the reliance of
23 a sector's business and operational functionality on cyber assets, systems, or networks. This methodology
24 involves using the NIPP baseline criteria, developing a sector-specific model of risk, and applying a cyber-
25 dependency screen to identify cyber assets, systems, and networks that may have nationally significant
26 consequences if lost. If a sector's cyber asset identification methodology already exists, DHS will work with
27 the sector to ensure alignment of that methodology with the NIPP risk management framework described in
28 Chapter 3.

29 DHS also has ongoing efforts to ensure that the National Asset Database (NADB) and other asset
30 description databases being utilized for CI/KR risk assessment contain appropriate information on cyber
31 assets, systems, and networks.

32 1A.3.3 Assess Risks

33 Risk assessment for cyber assets, systems, and networks is an integral part of the NIPP risk management
34 framework described in the NIPP. This framework combines consequences, threats, and vulnerabilities to
35 produce systematic, comprehensive, and defensible risk assessments. DHS and the SSAs assess risk for
36 cyber assets, systems, and networks associated with other CI/KR at the national and sector levels.

37 DHS will incorporate the results of these risk assessments in its overall risk management process to
38 prioritize where the Nation's limited resources for CI/KR protection activities should be applied.

1 **Consequence Analysis:** The first step in the risk assessment process involves determining the
2 consequences of destruction, incapacitation, or exploitation of an asset.

3 To assess whether a given asset may be nationally consequential, physical, cyber, and human asset
4 dependencies and interdependencies need to be assessed. Cyber interdependence presents a unique
5 challenge for all sectors because of the borderless nature of cyberspace. Interdependencies are dual in
6 nature – for example, the energy sector relies on computer-based control systems to manage the electric
7 power grid, while those same control systems require electric power to operate.

8 Sophisticated modeling and simulations through the National Infrastructure Simulation and Analysis Center
9 (NISAC) will help quantify national and international dependency and interdependency, and assess their
10 potential consequences. However, this effort is complex and time consuming, and may not be appropriate
11 for all assessments. When such advanced capability is not available, dependency and interdependency
12 analyses must be carried out in a more subjective manner, with the participation of subject matter experts
13 who have operational knowledge of the sectors involved, as well as the cross-sector interactions that are
14 likely.

15 The consequences of cyber asset, system, or network destruction, incapacitation, or exploitation must be
16 measured and described using a consistent system of measurements to ensure that the results can be
17 compared across sectors. The NIPP provides baseline criteria for assessment methodologies to ensure
18 such consistency. DHS also makes the Risk Analysis and Management for Critical Asset Protection
19 (RAMCAP) process available to various sectors for use at their discretion. While either of these approaches
20 enables the consistent assessment of cyber consequences, both require that cyber assets, systems, and
21 networks be properly accounted for in the analysis process for the results to properly assess the
22 consequences of cyber loss.

23 **Vulnerability Assessment:** The second step of the risk assessment process is analysis of vulnerability –
24 determining which elements of infrastructure are most susceptible to attack and how attacks against these
25 elements would be carried out.

26 DHS works to identify cross-sector best practices to ensure that the existing methodologies used by SSAs
27 and other security partners address cyber vulnerabilities and has taken a broad, inclusive approach by
28 reviewing various existing publicly available methods across government, industry, and academia, to
29 assemble a hybrid of the best practices. For example, DHS is not only examining vulnerability standards
30 from the International Organization for Standardization and the National Institute of Standards and
31 Technology, but is also studying higher level vulnerability assessment methods in use within the law
32 enforcement and intelligence communities.

33 DHS works to leverage well-established methodologies that have traditionally focused on physical
34 vulnerabilities by enhancing them to better address cyber elements. Examples of these efforts include the
35 enrichment of the Vulnerability Identification Self-Assessment Tool, as well as the RAMCAP process.

36 DHS will publish its best practices for cyber vulnerability assessments 120 days after the approval of the
37 NIPP.

38 **Threat Analysis:** The third step of the risk assessment process is the analysis of threat, which provides the
39 likelihood that a target will be attacked. There are increasing indicators that potential adversaries intend to

conduct cyber attacks and are actively acquiring cyber attack capabilities. Additionally, the increasing ease with which powerful cyber attack tools can be obtained and used puts the capability of conducting cyber attacks within reach of most groups or individuals who wish to do harm to the United States. However, credible information on specific adversaries is often not available. As such, DHS collaborates with the law enforcement and intelligence communities and the private sector to more accurately portray the possible ways in which the cyber threat may affect CI/KR, including the exploitation of the Internet as a weapon.

As called for in the National Strategy to Secure Cyberspace, DHS provides input on cyber-related issues for the National Intelligence Estimate of Cyber Threats to the U.S. Information Infrastructure. DHS will update its assessment on an annual basis to inform the general threat scenarios used in risk assessments and provide input to the National Intelligence Estimate as required.

1A.3.4 Prioritize

NIPP risk assessments provide comparable estimates of the risk faced by each element and sector of CI/KR; this allows elements and sectors to be prioritized according to their risk, and protective programs – including cyber programs – to be designed that can reduce the highest priority risk. The expected risk reduction and cost of the programs allow them to be prioritized for implementation on the basis of investment return – those programs that offer the greatest risk reduction for the dollars spent are the highest priority protective programs to be implemented. Cyber programs often prove to be highly cost-effective approaches for reducing risk.

Prioritization of programs based on cost and effectiveness ensures that the programs that support the NIPP make the greatest contribution possible to overall CI/KR risk reduction for the money that is invested in them. Cyber assets, systems, and networks are prioritized as part of the DHS overall risk-based approach to prioritization. By integrating cyber threats, vulnerabilities, and consequences into risk analysis, and by measuring risk in comparable terms for all elements and sectors, cyber assets, systems, and networks are included in the prioritization process in a manner that ensures that they are appropriately considered along with other aspects of CI/KR.

1A.3.5 Implement Protective Programs

DHS recognizes that each sector will have a unique reliance on cyber infrastructure and, therefore, will assist the SSAs in developing a range of effective and appropriate cyber-protective measures.

In addition to individual sector-level protective measures, DHS has partnered with other public and private sector entities to develop and implement specific programs to help build a national cyberspace security response system that supports NIPP cyber risk reduction:

- **Government Forum of Incident Response and Security Teams (GFIRST):** The Federal interagency community established the GFIRST to facilitate interagency information sharing and cooperation across Federal agencies for readiness and response efforts. GFIRST is a group of technical and tactical security response team practitioners responsible for securing government information technology systems. The members work together to understand and handle computer security incidents and to encourage proactive and preventive security practices.

- 1 • **Internet Disruption Working Group:** DHS coordinates cybersecurity contingency plans, including a
2 plan for recovering Internet functions. To meet this need, DHS formed a strategic partnership with the
3 Internet Disruption Working Group in January 2005 to combine resources, avoid duplication of effort,
4 and leverage past Federal government, academic, and private sector work. The group assesses the
5 operational dependency of critical infrastructure sectors on the Internet, and collaborates with major
6 security partners to identify and prioritize the short-term protective measures necessary to prevent
7 major disruptions of the Internet or reduce their consequences, and to identify responsive/reconstitutive
8 measures for contingency plans in the event of a major disruption. The Internet Disruption Working
9 Group also assesses the likelihood of a disruption within operationally dependent sectors, and
10 determines where vulnerability assessments are most needed. This group has also reviewed previous
11 Internet disruption reports to identify high-priority actions to quickly and effectively improve the
12 resiliency of the Internet.
- 13 • **National Cyber Exercises:** DHS conducts exercises to identify, test, and improve coordination of the
14 cyber incident response community, including Federal, State, local, tribal, and international government
15 elements, as well as private sector corporations and coordinating councils. The most comprehensive of
16 these exercises is the National Cyber Exercise "Cyber Storm." The main objectives of Cyber Storm are
17 to practice effective collaborative response to a variety of cyber attack scenarios, including crisis
18 decision making; provide an environment for evaluation of interagency and inter-sector business
19 processes that rely on the information infrastructure; measure the progress of ongoing U.S. efforts to
20 defend against and respond to attacks; and foster improved information sharing among government
21 agencies and between government and private industry. The Cyber Storm exercises also sensitize a
22 diverse constituency of private and public sector decision makers to a variety of potential cyber threats,
23 including strategic attacks; familiarize this constituency with the national cyber response system and
24 the importance of their role in it; and practice the roles and responsibilities of government agencies and
25 industry in cyber incident response. Weaknesses discovered in government-wide processes during
26 exercises will be included in agency corrective action plans and are submitted to the Office of
27 Management and Budget (OMB).
- 28 • **The National Cyber Response Coordination Group:** The National Cyber Response Coordination
29 Group facilitates coordination of the Federal government's efforts to prepare for, respond to, and
30 recover from cyber Incidents of National Significance and other national cyber incidents and physical
31 attacks that have significant cyber consequences (collectively known as "cyber incidents"). It serves as
32 the Federal government's principal interagency mechanism for operational information sharing and
33 coordination of Federal government response and recovery efforts during a cyber crisis. During such
34 incidents, the National Cyber Response Coordination Group member agencies coordinate their
35 capabilities to assess the domestic and international scope and severity of a cyber incident. The
36 member agencies use their situational awareness of a cyber incident to govern response and
37 remediation efforts and to guide senior policymakers. The member agencies also develop, coordinate,
38 and recommend courses of action and incident response strategies for the U.S. government. Moreover,
39 the member agencies use their established relationships with the private sector and State, local, and
40 tribal governments to help manage a cyber crisis, develop courses of action, and devise response and
41 recovery strategies.
- 42 • **Programs for Federal Systems Cybersecurity:** Federal agencies prevention and protection efforts
43 include those that are focused on securing their own cyber infrastructure. HSPD-7 mandates that "the
44 heads of all Federal departments and agencies shall develop and submit to the Director of the Office of

Management and Budget (OMB) for approval plans for protecting the physical and cyber CI/KR that they own or operate. These plans shall address identification, prioritization, protection, and contingency planning, including the recovery and reconstitution of essential capabilities." To assist Federal agencies in their efforts, DHS acts as subject matter expert to OMB in reviewing the cyber aspects of Federal agency CI/KR plans to ensure that cyber risk is addressed consistently across all Federal agencies. DHS is works with the OMB to improve Federal civilian agencies' cybersecurity posture and compliance with the Federal Information Security Management Act (FISMA).

DHS, in collaboration with other security partners, has also established several vulnerability-reduction programs under the NIPP risk management framework, including:

- **Control Systems Security:** Control systems are computer-based systems used within many infrastructures and industries to monitor and control sensitive processes and physical functions. Control systems typically collect measurement and operational data from the field, process and display the information, and relay control commands to local or remote equipment or human-machine interfaces (operators). Control systems are embedded throughout the Nation's CI/KR (e.g., chemical, manufacturing, water treatment, and food processing plants, transportation systems, oil and gas refineries, power generation plants, and transmission systems). They are frequently implemented with remote access and open connectivity, which exposes them to increasing cyber threats that could have a devastating impact on national security, economic security, and public health and safety, as well as the environment. The DHS Control Systems Security Initiative coordinates efforts among Federal, State, local, and tribal governments, as well as control system owners, operators, and vendors to improve control system security within and across all critical infrastructure sectors. DHS also leads a comprehensive national initiative to implement protection of control systems through the production and timely dissemination of situational awareness information to convey the "state of security" of the Nation's critical control systems. DHS created the U.S. Computer Emergency Readiness Team (US-CERT) Control Systems Security Center (CSSC) that develops and implements programs aimed at reducing the likelihood of success and the severity of the impact of a cyber attack against critical infrastructure control systems. The CSSC coordinates government and industry activities to identify and mitigate control systems vulnerabilities, perform vulnerability assessments, and provide a national response capability for control systems incidents.
- **Software Assurance Program:** Public and private sector security partners work together to develop best practices and new technologies to promote integrity, security, and reliability in software development. DHS leads the Software Assurance Program, a comprehensive software assurance strategy that addresses people, processes, technology, and acquisition throughout the software development life cycle. The DHS efforts to achieve a broader ability to routinely develop and deploy trustworthy software products and ensure the continued competitiveness of the U.S. software industry through public-private partnerships are a significant element of securing cyberspace and the Nation's critical infrastructure. These efforts will lead to the production of higher quality, more secure software. The overall goal is secure and reliable software supporting mission requirements, enabling more resilient organizations.

The Software Assurance Program is designed to lead the development of practical guidance and review tools, and promote R&D investment in cybersecurity. As part of its efforts, DHS co-sponsors the National Vulnerability Database, a set of centralized and comprehensive vulnerability information in order to assist

with incident prevention and management (including patches) to mitigate consequences and vulnerabilities. Additionally, the program is conducting a comprehensive review of the National Information Assurance Partnership to determine the extent to which it adequately addresses security flaws. The National Information Assurance Partnership promotes the development of sound security requirements for IT products and systems, as well as appropriate security evaluation metrics.

Examples of other Federal agencies' cybersecurity access control, certification, and policy enforcement tools that support NIPP cyber risk management include:

- **The General Services Administration (GSA)** is responsible for developing and implementing a government-wide infrastructure for authentication services. In March 2004, GSA began to develop an automated risk assessment tool for government-wide use in certifying and accrediting its eAuthentication gateway. In addition, GSA is creating a list of approved solution providers that supply smart cards based on Federal Public Key Infrastructure standards and that include a new electronic authentication policy specification.
- **The National Oceanic and Atmospheric Administration** has implemented enterprise-wide vulnerability assessments, an intrusion detection system, enterprise-wide virus detection software to enforce security policy, anti-virus scanning gateways, and a patch management policy.

1A.3.6 Measure Effectiveness and Improve Programs

There are several critical infrastructure core cyber measures and metrics that will be tracked across each sector to enable comparison and analysis between and among different types of critical infrastructure. The cyber core measures and metrics will mirror the core measures and metrics being developed for the NIPP, but will also include the review, consideration, and integration of common cybersecurity standards. Examples of how these measures and metrics are customized for cyber assets, systems, and networks are provided in Table 1A-1.

Table 1A-1: Sample Cyber Measures and Metrics

Cyber Measure	Description
Total number of cyber assets, systems, and networks.	This descriptive cyber data will be collected for each sector.
Number of cyber assets, systems, and networks with potential for medium or high consequences.	Tracking this measure will help determine which sectors are in the most need of assessing cyber vulnerabilities and whether there are particularly critical regions or industries. This measure could be an outcome if protective actions intend to devalue assets to reduce potential consequences if they are compromised.
Percentage of medium- or high-consequence cyber assets, systems, and networks with completed vulnerability analyses.	Tracking this measure will help determine progress in determining which infrastructure assets and sectors are in the most need of protective and preventive programs.
Percentage of medium- or high-consequence cyber assets, systems, and networks assessed as high risk.	Tracking this will help in determining which sectors require programs to increase preventive, protective, response, and recovery capabilities. In conjunction with other measures and data on location and ownership of the assets, it can help focus government and private resources on those sectors, regions, and industries with the highest identified risks first.

Table 1A-1: Sample Cyber Measures and Metrics *(continued)*

Cyber Measure	Description
Percentage of medium- or high-consequence cyber assets, systems, and networks that have active protective programs to measurably reduce risk.	Tracking this, in conjunction with other measures, will help determine where there are potential gaps in program coverage for critical infrastructure cyber assets determined to be high risk.
Percentage of medium- or high-consequence cyber assets, systems, and networks that have been assessed for readiness, response, and recovery capability.	Tracking this measure will provide insight into the effectiveness of cyber readiness, response, and recovery.
Percentage of cyber assets, systems, and networks reduced from high risk.	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. For example, programs can reduce risk by 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 measures.

Once the core metrics have been developed and approved, a data-gathering and reporting process will be established in order to identify the necessary individuals and information for measuring progress. As each sector's available data can differ, this process will have to take into consideration any unique situations that may arise. This process will outline, but will not be limited to, the responsible parties, data collection and reporting methodology, and timeframes for data and metrics submissions. Additionally, as the process matures, additional metrics will be considered to reflect the most important issues currently being faced by the sectors.

The overall purpose of measuring effectiveness using metrics is to improve cyber CI/KR protection by reducing risk. This means that using metrics as descriptors is not sufficient and that measured effectiveness must be compared to goals and improvements made where there are shortfalls.

1A.4 Ensuring Long-Term Cybersecurity

The effort to ensure a coherent cyber CI/KR protection program over the long term has four components that are described in greater detail below:

- **Information Sharing and Awareness:** Ensures implementation of effective, coordinated, and integrated CI/KR protection efforts of cyber assets, systems, and networks, and enables cybersecurity partners to make informed decisions with regard to short- and long-term cybersecurity postures, risk mitigation, and operational continuity.
- **International Cooperation:** Promotes a global culture of cybersecurity and improves overall cyber incident preparedness and response posture.
- **Training and Education:** Ensures that skilled and knowledgeable cybersecurity professionals are available to undertake NIPP programs in the future.

- **Research and Development:** Improves cybersecurity protective capabilities or dramatically lowers the costs of existing capabilities so that State, local, tribal, and private sector security partners can afford to do more with their limited budgets.

1A.4.1 Information Sharing and Awareness

Information sharing and awareness involves sharing programs with agency partners and other security partners and special sharing arrangements for emergency situations. Each of these is discussed below.

Interagency Coordination: Interagency cooperation and information sharing are essential to improving the national cyber counterintelligence and law enforcement capabilities. The intelligence and law enforcement communities have both official and informal mechanisms in place for information sharing that DHS supports:

- **Computer Crime and Intellectual Property Section,** the FBI, and the U.S. Secret Service meet regularly to coordinate and resolve conflicts in investigations, ensuring that there is no duplication of effort.
- **Cybercop Portal** is a secure Internet-based information-sharing mechanism for more than 5,300 law enforcement members involved in the field of electronic crimes investigations. The law enforcement community, including investigators from private industry (e.g., banks and the network security community), is tied together and supported by this secure, Internet-based, collaboration portal.
- **FBI's InfraGard** program is a public-private partnership coordinated out of the 56 FBI field offices. The program brings together law enforcement, academia, and private sector entities on a monthly basis to provide a forum for information sharing and networking.
- **FBI's Inter-Agency Coordination Cell** is a multi-agency group focused on sharing law enforcement information on cyber-related investigations.
- **U.S. Secret Service's Electronic Crime Task Forces** provide interagency coordination on cyber-based attacks and intrusions.

Cybersecurity Awareness for Security Partners: DHS has a leadership role in coordinating a public-private partnership to promote and raise cybersecurity awareness among the general public by:

- Partnering with other Federal and private sector organizations to sponsor the National Cyber Security Alliance (NCSA);
- Creating a public-private organization, Stay Safe Online, to educate home users, small businesses, and K-12 and higher education audiences on cybersecurity best practices; and
- Collaborating with the public and private sector to establish October as "National Cyber Security Awareness Month" and participating in activities to raise awareness of cybersecurity nationwide.

Cyberspace Emergency Readiness: DHS established the US-CERT, which is a 24/7 single point of contact for cyberspace analysis warning, information sharing, and incident response and recovery for a broad range of users, including government, enterprises, small businesses, and home users. US-CERT is a partnership between DHS and the public and private sectors designed to protect the Nation's Internet

1 infrastructure and to coordinate defenses against and responses to cyber attacks across the Nation. US-
2 CERT is responsible for:

- 3 • Analyzing and reducing cyber threats and vulnerabilities;
- 4 • Disseminating cyber threat warning information; and
- 5 • Coordinating cyber incident response activities.

6 To support the information-sharing requirements of the networked approach, US-CERT provides the
7 following information on their Web site, accessible via the Homeland Security Information Network (HSIN),
8 and via mailing lists:

- 9 • **Cybersecurity Alerts:** Written in a language for home, corporate, and new users, these alerts are
10 published in conjunction with technical alerts when there are security issues that affect the general
11 public.
- 12 • **Cybersecurity Bulletins:** Bulletins summarize information that has been published on new security
13 issues and vulnerabilities. They are published weekly and are written primarily for systems
14 administrators and other technical users.
- 15 • **Cybersecurity Tips:** Tips provide information and advice about a variety of common cybersecurity
16 topics. They are published biweekly and are written primarily for home, corporate, and new users.
- 17 • **National Web Cast Initiative:** In an effort to increase cybersecurity awareness and education among
18 the States, DHS, through US-CERT, and the Multi-State Information Sharing and Analysis Center have
19 launched a joint partnership to develop a series of national Web casts that will examine critical and
20 timely cybersecurity issues. The purpose of the initiative is to strengthen the Nation's cyber readiness
21 and resilience.
- 22 • **Technical Cybersecurity Alerts:** Written for systems administrators and experienced users, technical
23 alerts provide timely information about current cybersecurity issues, vulnerabilities, and exploits.

24 US-CERT also provides a method for citizens, businesses, and other institutions to communicate and
25 coordinate directly with the U.S. government on matters of cybersecurity. The private sector can use the
26 protections afforded by the Protected Critical Infrastructure Information Act to electronically submit
27 proprietary data to US-CERT.

28 **1A.4.2 International Coordination on Cybersecurity**

29 The U.S. government proactively uses its intelligence capabilities to protect the country from cyber attack,
30 its diplomatic outreach and operational capabilities to build partnerships in the global community, and its
31 law enforcement capabilities to combat cyber crime wherever it originates. The private sector, international
32 industry associations, and companies with global interests and operations are also engaged in addressing
33 cybersecurity internationally. For example, the U.S.-based Information Technology Association of America
34 participates in international cybersecurity conferences and forums, such as the India-based National
35 Association for Software and Service Companies Joint Conference. These efforts require interaction with
36 both policy and operational functions to coordinate national and international activity that is mutually
37 supportive across the globe:

- 1 • **International Cybersecurity Outreach:** DHS, in cooperation with the Department of State and other
2 Federal agencies, engages in multilateral and bilateral discussions to further international security
3 awareness and policy development, as well as incident response team information-sharing and
4 capacity-building objectives. DHS engages in bilateral discussions on important cybersecurity issues
5 with countries of interest, including Norway, Italy, Egypt, Israel, India, Japan, and others. DHS also
6 provides leadership in multilateral and regional forums addressing cybersecurity and critical information
7 infrastructure protection. For example, the Asia Pacific Economic Cooperation (APEC)
8 Telecommunications Working Group (TEL) has engaged in a capacity-building program to help
9 member countries develop computer emergency response teams. The Organization of American
10 States (OAS) has approved a framework proposal by its Cyber Security Working Group to create an
11 OAS regional computer incident response points-of-contact network for information sharing and
12 capacity building. Multilateral collaboration to build a global culture of security includes participation in
13 the Organization for Economic Cooperation and Development (OECD), the G8, and the United Nations.
14 Many of these countries and organizations have developed mechanisms for engaging the private
15 sector in their dialog and program efforts, and the U.S. private sector has been actively involved.
- 16 • **Collaboration on Cyber Crime:** The U.S. outreach strategy for comprehensive cyber laws and
17 procedures draws on the Council of Europe Convention on Cyber Crime, as well as: (1) the G8 High-
18 Tech Crime Working Group's principles for fighting cyber crime and protecting critical information
19 infrastructure, (2) the OECD guidelines on information and network security, and (3) the United Nations
20 General Assembly resolutions based on the G8 and OECD efforts. The goal of this outreach strategy is
21 to encourage individual nations and regional groupings of nations to join DHS in efforts to protect the
22 internationally interconnected national systems.
- 23 • **Collaborative Efforts for Cyber Watch, Warning, and Incident Response:** The United States is
24 working strategically with key allies on cybersecurity policy and operational cooperation. Leveraging
25 pre-existing relationships among Computer Security Incident Response Teams (CSIRTs), DHS has
26 established a preliminary framework for cooperation on cybersecurity policy, watch, warning, and
27 incident response with key allies (Australia, Canada, New Zealand, and the United Kingdom). The
28 framework also incorporates efforts related to key strategic issues as agreed upon by these allies. DHS
29 is also considering and participating in the establishment of an International Watch and Warning
30 Network (IWWN) among cybersecurity policy, computer emergency response, and law enforcement
31 participants of 15 countries. The IWWN will provide a mechanism for the participating countries to
32 share information to build global cyber situational awareness and coordinate incident response.
- 33 • **Partnerships to Address Cyber Aspects of Critical Infrastructure Protection:** DHS is leveraging
34 existing agreements such as the Security and Prosperity Partnership of North America (SPP) and the
35 Joint Contact Group (JCG) with the United Kingdom to address the IT Sector and cross-cutting cyber
36 components of critical infrastructure protection. The trilateral SPP builds on existing bilateral
37 agreements between the United States and Canada and the United States and Mexico by allowing
38 issues to be addressed on a dual bi-national basis. In the context of the JCG, DHS established a 10-
39 point action plan to address cybersecurity, watch, warning, and incident response and other strategic
40 initiatives.

1A.4.3 Training and Education

The National Strategy to Secure Cyberspace highlights the importance of cyberspace security training and education. Education and training are strategic initiatives in which DHS and other Federal agencies are actively engaged to affect a greater awareness and participation in efforts to promote cybersecurity for the future.

The Federal government has undertaken several initiatives in partnership with research and academic communities to better educate and train future cybersecurity practitioners:

- DHS co-sponsors the National Centers of Academic Excellence in Information Assurance Education program with the National Security Agency. Together, DHS and the National Security Agency are working to expand the program nationally.
- DHS collaborates with the National Science Foundation (NSF) to co-sponsor and expand the Scholarship for Service program (known as the Cyber Corps program). The Scholarship for Service program provides grant money to selected Centers of Academic Excellence in Information Assurance Education and other universities with programs of a similar caliber to fund the final two years of students' bachelor's, master's, or doctoral study in information assurance in exchange for an equal amount of time spent working for the Federal government.
- In fiscal year 2004, the joint DHS/Treasury Computer Investigative Specialist program trained 48 Federal criminal investigators in basic computer forensics. The agents from ICE, the Internal Revenue Service, and the U.S. Secret Service attended the basic six-and-a-half-week course. This training was funded through the Treasury Executive Office of Asset Forfeiture. In fiscal year 2005, schools are scheduled for 72 more Federal investigators and 80 State and local officers.
- DHS is collaborating with the Department of Defense to finalize a comprehensive IT job skills standard to guide development of a national certification program for security professionals within the Federal government and private industry.

1A.4.4 Research and Development

The Cyber Security Research and Development Act of 2002 authorized a multiyear effort to create more secure cyber technologies, expand cybersecurity R&D, and improve the cybersecurity workforce.

To further address cyber R&D needs, the White House Office of Science and Technology Policy (OSTP) established a Cyber Security and Information Assurance Interagency Working Group under the National Science and Technology Council (NSTC). The Cyber Security and Information Assurance Interagency Working Group was jointly chartered by NSTC's Subcommittee on Networking and Information Technology Research and Development and the Subcommittee on Infrastructure. This interagency working group includes participation from 20 organizations in 11 departments and agencies, as well as from several offices in the White House.

The purpose of the working group is to coordinate policy, programs, and budgets for cybersecurity and information assurance R&D. The Cyber Security and Information Assurance Interagency Working Group currently is engaged in developing the Federal Plan for Cybersecurity R&D, which includes near-term, mid-term, and long-term cybersecurity research efforts in response to the National Strategy to Secure

- 1 Cyberspace and HSPD-7. Specific examples include efforts to improve the security of control systems,
- 2 fundamental protocols (such as Internet Protocol Version 6), and authentication technologies, and to
- 3 periodically review emerging technologies. DHS actively participates in Cyber Security and Information
- 4 Assurance Interagency Working Group activities and continues to identify critical cyber R&D requirements
- 5 for incorporation into Federal R&D planning efforts.

Appendix 1B: International CI/KR Protection

1B.1 Introduction and Purpose of This Appendix

This appendix provides guidance for addressing the international aspects of CI/KR protection in support of the NIPP.

1B.1.1 Scope

The NIPP provides the mechanisms, processes, key initiatives, and milestones required for DHS, the Department of State, the SSAs, and other security partners to address international implications and requirements related to CI/KR protection. The NIPP and associated SSPs recognize that protective measures do not stop at a facility's fence line or a national border. Because disruptions in the global infrastructure can ripple and cascade around the world, the NIPP and SSPs also must consider cross-border infrastructure, international vulnerabilities, and global and sector dependencies and interdependencies.

1B.1.2 Vision

The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets identifies "fostering international cooperation" as one of the eight guiding principles of its vision for the future. The Strategy underscores the need for a coordinated, comprehensive, and aggressive global action as a key aspect of the NIPP approach to CI/KR protection.

Furthermore, the National Strategy to Secure Cyberspace sets forth strategic objectives for National Security and International Cyberspace Security Cooperation that deal directly with the international aspects of CI/KR protection, including preventing cyber attacks against America's critical infrastructure, reducing vulnerabilities, and minimizing damages and recovery time from cyber attacks that do occur.

1B.1.3 Implementing the Vision With a Strategy for Effective Cooperation

The NIPP CI/KR international coordination and protection strategy outlined in this appendix is focused on instituting effective *cooperation with international security partners*, rather than on *specific protective measures*. Specific protective measures are tailored to each sector's particular circumstance and are developed in SSPs. This appendix also focuses on implementing existing agreements that affect CI/KR protection and on addressing cross-sector and global issues such as cybersecurity.

The Department of State and DHS will periodically review the international Critical Infrastructure Protection Strategy and redraft it, as needed, to ensure that it complements and supports international CI/KR protection issues specified by the NIPP.

Within six months of the approval of the NIPP, DHS, the Department of State, and other concerned Federal agencies will incorporate the NIPP into their strategies for cooperating with other countries and international/multinational organizations with the purpose of promoting a global culture of physical security and cybersecurity, as well as promoting an international strategy that will manage the risk as far as possible outside the United States' physical borders; accelerate international cooperation to develop intellectual

infrastructure based on shared assumptions and compatible conceptual tools; and connect constituencies not traditionally engaged in security. The broad structure of this strategy is outlined in this appendix; it is based on the following high-level considerations.

1B.2 Responsibilities for International Cooperation on CI/KR Protection

In accordance with HSPD-7, the Department of State, in conjunction with DHS; the Departments of Justice, Commerce, Defense, and Treasury; the Nuclear Regulatory Commission; and other appropriate agencies, is responsible for working with foreign countries and international/multinational organizations to strengthen the protection of U.S. CI/KR. This section provides further details regarding the responsibilities of DHS and other security partners related to the international dimension of CI/KR protection.

1B.2.1 Department of Homeland Security

Under the CI/KR risk management framework described in this Plan, DHS is responsible for the following actions, all of which have an international dimension:

- Building security partnerships;
- Implementing a comprehensive, integrated risk management program; and
- Implementing protective programs.

DHS, in conjunction with the Department of State and other appropriate U.S. government agencies, will share with international entities appropriate information and perform outreach functions to enhance information sharing and management of international agreements regarding CI/KR protection.

Some of the more complex challenges presented by the international aspects of CI/KR protection involve analyzing the complex dependencies, interdependencies, and vulnerabilities that require the application of sophisticated and innovative modeling techniques to assess. DHS is responsible for pursuing research and analysis in this area. It will call on a range of outside sources for this work, including those with expertise in the international community and the National Infrastructure Simulation and Analysis Center (NISAC).

1B.2.2 Department of State

The Secretary of State has direct responsibility for policies and activities related to the protection of U.S. citizens and U.S. facilities abroad. The Secretary of State, in conjunction with the Secretary of Homeland Security, is responsible for coordinating with foreign countries and international organizations to strengthen the protection of U.S. CI/KR. The Department of State supports DHS and other Federal agency efforts by providing knowledge about and access to other governments. The Department of State leverages bilateral and multilateral relationships around the world to ensure that the U.S. government can act effectively in identifying and protecting U.S. CI/KR.

The Department of State, DHS, and other agencies are engaged in a wide range of activities throughout the world to prevent, disrupt, and deter threats and acts of terrorism directed against the homeland and U.S. interests abroad. The objectives of these efforts are to develop and work with global partners to ensure mutual security and to raise awareness of the terrorist threat.

1B.2.3 Other Federal Agencies

SSAs exchange information, including cyber-specific information, with security partners in other countries, in accordance with guidelines established by DHS and Department of State and other agencies, as appropriate, to improve the Nation's overall CI/KR protection posture.

The departments of Justice, Commerce, Defense, Treasury, and other departments share responsibility, in accordance with HSPD-7, for working with foreign countries and international organizations to strengthen the protection of U.S. CI/KR.

1B.2.4 State, Territorial, Local, and Tribal Governments

State and Territorial governments ensure ongoing cooperation with relevant international, regional, local and private sector CI/KR protection efforts.

1B.2.5 Private Sector

DHS is working with the private sector, SSAs, private voluntary and non-governmental organizations, and information-sharing mechanisms and organizations to protect cross-border infrastructure and understand international and global vulnerabilities. DHS relies on the private sector for data, expertise, and knowledge of their international operations to identify relevant international assets and assess risks and global vulnerabilities, including shared threats and interdependencies.

1B.2.6 Academia

The academic community provides data, insight, and research into the significance of international interdependencies, modeling, and analysis, and uncovers previously unknown nodes, behaviors, and vulnerabilities.

1B.3 Managing the International Dimension of CI/KR Risk

The NIPP addresses international CI/KR protection, including interdependencies and the vulnerability to threats that originate outside the country. The NIPP brings a new focus to international security cooperation, and provides a risk-based strategic framework for measuring the effectiveness of international CI/KR protection activities. The NIPP also provides tools to assess international vulnerabilities and interdependencies that complement long-standing cooperative agreements with Canada, Mexico, the United Kingdom, NATO, and others, and provides a framework for effective collaborative engagement with additional international partners.

SSPs are required to include international considerations as an integral part of each sector's planning process rather than instituting a separate layer of planning. Some international aspects of CI/KR protection require additional overarching or cross-sector emphasis. These include:

- U.S. interaction with foreign governments and international organizations to enhance the confidentiality, integrity, and availability of cyber-based infrastructures that often have an international or even global dimension;

- Protection of physical assets located on or near the borders with Canada and Mexico requiring cooperation with and/or planning and resource allocation among neighboring countries, States bordering on these countries, and affected local and tribal governments;
- Sectors with infrastructure that is extensively integrated into an international or global market (e.g., financial services or other information-based business, energy, or transportation) or when the proper functioning of a sector relies on inputs that are not within the control of U.S. entities; and
- U.S. government and corporate facilities located overseas that may be regarded as CI/KR may be determined to be critical based on implementation of the NIPP framework. Protection for the Government Facility Sector involves careful *interagency* cooperation, as well as cooperation with foreign CI/KR security partners.

The following subsections discuss issues associated with the international aspects of CI/KR protection in the context of the steps of the NIPP risk management process. (See NIPP Chapter 3, The Protection Program Strategy: Reducing Risk.)

1B.3.1 Setting Security Goals

The overarching goal of the NIPP – to enhance the Nation’s protection of U.S. CI/KR – applies to the international “system of systems” that underpins U.S. CI/KR. The NIPP and the SSPs provide goals and protective actions that address the international aspects of CI/KR protection effort on a sector-specific basis. In addition, a separate set of goals and priorities guide cross-sector efforts to improve protection for CI/KR with international linkages. These goals fall into three categories:

- Identifying and addressing cross-sector and global issues;
- Implementing existing and developing new agreements that affect CI/KR; and
- Improving the effectiveness of international cooperation.

DHS, in conjunction with the Department of State and other security partners, will define a comprehensive international CI/KR protection strategy for pursuing and achieving these goals in ways that complement each other and are achievable with the resources available.

Important considerations in achieving these goals are discussed in this section; actions required to achieve these goals are addressed in the section on key implementation actions below.

1B.3.2 Identifying Assets Affected by International Linkages

Once international security goals are set, the next step in the risk management process is to develop and maintain a comprehensive inventory of the Nation’s CI/KR outside the U.S. borders and of foreign CI/KR that may affect systems within this country. The process for identifying nationally critical assets involves working with U.S. industry, SSAs, academia, and international partners to gather and protect information on the foreign infrastructure and resources on which U.S. CI/KR relies.

Dependency and Interdependency and International CI/KR Protection Cooperation: The NIPP risk management framework details a structured approach for use in determining dependencies and

interdependencies, including physical, cyber, and international considerations. This approach is designed to address CI/KR protection in three areas:

- Direct international linkages to physical and cyber U.S. CI/KR:
 - Foreign cross-border assets linked to U.S. CI/KR, such as roads, bridges, pipelines, gas lines, telecommunication lines and undersea cables and facilities, and power lines, etc., physically connecting U.S. CI/KR to Canada and Mexico;
 - Foreign infrastructure whose disruption or destruction could directly harm the U.S. homeland, such as waters behind a Canadian dam that could flood U.S. territory and a toxic plume from a destroyed Mexican chemical plant that could contaminate U.S. territory; and
 - U.S. CI/KR that may be located overseas, such as non-military government facilities, are overseas components of U.S. CI/KR;
- Indirect international linkages to physical and cyber U.S. CI/KR:
 - The potential cascading and escalating effects of disruption or destruction of foreign assets, systems, and networks; critical foreign technology; goods; resources; transit routes; and chokepoints; and
 - Foreign ownership, control, or involvement in U.S. CI/KR and related issues; and
- Global aspects of physical and cyber U.S. CI/KR:
 - Infrastructure assets either located around the world or with global mobility that require the efforts of multiple foreign countries to secure.

Dependency and interdependency analysis is primarily based on information from each sector and is formulated by the judgments of CI/KR owners and operators regarding their supply chains and sources of other services from other infrastructure sectors, such as power and water. As the capability for sophisticated network analysis grows, these inputs will be complemented by assessments that examine less apparent network-based dependencies and interdependencies. The National Infrastructure Simulation and Analysis Center (NISAC) supports this effort by analyzing and quantifying national and international dependency and interdependency for complex systems and networks that affect specific sectors.

1B.3.3 Assessing Risks

The risk assessment for CI/KR assets and systems that are affected by international linkages is an integral part of the risk management framework described in the NIPP. The risk management framework combines consequences, threats, and vulnerabilities to produce systematic and comprehensive risk assessments that can be clearly explained in a three-step process:

- Determining the consequences of destruction, incapacitation, or exploitation of an asset. This is done to assess potential national significance, as well as physical, cyber, and human dependencies and interdependencies that may result from international linkages.
- Analyzing vulnerability, including determining which elements of infrastructure are most susceptible to attack and whether attacks against these elements could be a consequence of any international linkages.

- Conducting a threat analysis that provides the likelihood that a target will be attacked. CI/KR with international linkages may present greater opportunities for attack and thus increase the likelihood that they may be the subject of attacks.

Issues important to the other countries may be different from those for the United States. Risk analysis needs to be conducted in coordination with other countries in order to draw upon their analysis, as well as our own.

1B.3.4 Prioritizing

Assessing assets on a level playing field that adjudicates risk based on a common framework ensures that resources are applied where they offer the most benefit for reducing risk, deterring threats, and minimizing the consequences of attacks. The same prioritization used for domestic CI/KR protection is observed to evaluate the risk arising from international linkages. The priority for protection investments could be raised if international linkages increase the risk.

1B.3.5 Implementing Programs

The SSAs have primary responsibility for developing protective measures that address risks that arise from international factors. In addition to sector protective measures, DHS has specific programs to help enhance the cooperation and coordination needed to address the unique challenges posed by the international aspects of CI/KR protection:

- **International Outreach Program:** DHS works with the Department of State and other relevant U.S. government agencies to conduct international outreach with foreign countries and international organizations to encourage the promotion and adoption of organization and policymaking structures, information-sharing mechanisms, industry partnerships, best practices, training, and other programs as needed to improve the protection of overseas assets and the reliability of foreign infrastructures on which the United States depends.
- **The National Cyber Response Coordination Group (NCRCG):** The NCRCG facilitates coordination of the Federal government's efforts to prepare for, respond to, and recover from cyber incidents of National Significance and other national cyber incidents and physical attacks that have significant cyber consequences (collectively known as "cyber incidents"). It serves as the Federal government's principal interagency mechanism for operational information sharing and coordination of Federal government response and recovery efforts during a cyber incident of national significance. NCRCG considers and consults with international partners on a regular basis for situational awareness and during such incidents. NCRCG member agencies integrate their capabilities to assess the domestic and international scope and severity of a cyber incident.
- **The National Exercise Program:** DHS provides overarching coordination for the National Exercise Program to ensure the Nation's readiness to respond in an all-hazards environment and to test the steady-state protection plans and programs put in place by the NIPP. The exercise program, as appropriate, engages international partners to address cooperation and cross-border issues, including those related to CI/KR protection. DHS and other security partners also participate in exercises sponsored by international partners, including cross-border, multi-sector tabletops.

- **National Cyber Exercises:** DHS is conducting exercises to identify, test, and improve coordination of the cyber incident response community, including Federal, State, Territorial, local, tribal, and international government elements, as well as private sector corporations and coordinating councils.

Because of the nature of the international dimension of CI/KR, a substantial emphasis is placed on standards that can be used to improve cooperation and coordination. To this end, DHS will lead efforts to:

- Collaborate to establish global standards, successful protection measures, and best practices related to telecommunications, air transportation systems, container shipping, cybersecurity, and other global systems as appropriate;
- Encourage the development and adoption of, and adherence to, standards of the International Organization for Standards and similar organizations that can help to reduce insurance premiums and level CI/KR protection costs for businesses; and
- Work with international security partners to determine the appropriate threshold for engagement with countries on cyber issues.

1B.3.6 Measuring Effectiveness and Making Improvements

The NIPP specifies three types of quantitative indicators to measure program effectiveness:

- **Descriptive Metrics** are necessary to understand sector resources and activity; they do not reflect CI/KR protection performance;
- **Process Metrics** measure whether specific activities were performed as planned; these track the progression of a task or report on the completion of an enabling process, such as forming a bilateral partnership; and
- **Outcome Metrics** track progress toward a strategic goal by beneficial results rather than level of activity.

The NIPP also distinguishes between two groups of metrics: core metrics that enable comparison and analysis between and among different sectors and sector-specific metrics that are useful within a sector.

Because protective measures are designed, implemented, and evaluated through sector-specific mechanisms guided by the SSPs, they deal with the protection challenges for a particular facility, network, or sector rather than international issues that may affect protection measures. Conversely, most initiatives that address the international issues affecting CI/KR protection are enablers rather than protective measures themselves. As a result, the metrics used to measure the effectiveness of international CI/KR protection initiatives will primarily be process metrics in the core group of CI/KR protection metrics. These will measure progress on tasks that enable CI/KR protection in situations that have international ramifications.

These metrics will be used to manage the comprehensive international CI/KR protection strategy, which enables SSP protection initiatives, and to track progress toward the strategy's three goals:

- Improving the effectiveness of international cooperation;

- Implementing existing and developing new agreements that affect CI/KR; and
 - Addressing cross-sector and global issues.
- DHS, in cooperation with other Federal agencies, will develop the metrics to track progress on international CI/KR protection enablers. Examples of such metrics include:
- The international issues being faced by each sector, which of these affect multiple sectors and which issues are the most important;
 - The countries that should be involved in protection partnerships for each sector;
 - The number and type of bilateral and multinational agreements affecting CI/KR protection;
 - The nature, level of implementation, and effectiveness of bilateral and multinational agreements;
 - The sectors affected by each international partnership;
 - The number and type of outcomes enabled by an international initiative; and
 - Where possible, the specific CI/KR protection enhancements that are directly attributable to a particular international initiative.
- Once the core metrics have been developed and approved, DHS and its relevant security partners will establish a data-gathering and reporting process. This process will outline, but will not be limited to, responsibilities; data collection, reporting procedures, and timeframes; metrics calculation; and the schedule for computing and updating the metrics on a regular basis.

1B.4 Organizing International CI/KR Protection Cooperation

DHS, in conjunction with the Department of State and other Federal agencies, works with individual foreign governments, and regional and international organizations in partnership to enhance the protection of the Nation's CI/KR and to deny the exploitation of CI/KR assets. Potential partnerships depend on:

- Physical proximity to the United States or U.S. assets;
- Useful experience and information to be gained from other countries;
- Existing alliances, agreements, and high-level commitments;
- Critical supply chains and vulnerable nodes; and
- Interdependencies and networked technologies, and the need for a global "culture of security" to protect physical and cyber assets.

As international CI/KR protection partnerships mature, cooperative efforts will strengthen in two dimensions:

- Development of new partnerships with countries possessing useful experience and information regarding CI/KR protective efforts, as well as terrorism prevention, preparedness, response, and recovery; and

- Development of new international relations and institutions to protect global infrastructures and to address international interdependencies, networked technologies, and the need for a global culture of security to protect physical and cyber assets.

The coordination mechanisms supporting the NIPP create linkages between CI/KR protection efforts at the national, sector, State, Territorial, regional, local, tribal, and international levels. The entities and bodies that are involved with this coordination are diverse and depend on the specifics of the issues they address and other considerations as discussed in the following subsections.

1B.4.1 Domestic Aspects of International CI/KR Protection Cooperation

Interagency Coordination – Department of State and DHS Leadership: DHS will work with the Department of State, international partners, and with U.S. entities involved with the international aspects of CI/KR protection to exchange experiences, share information, and develop a cooperative atmosphere to materially improve U.S. critical infrastructure protection, information sharing, cybersecurity, and global telecommunications standards. DHS and SSAs will work with specific countries to identify international interdependencies and vulnerabilities. SSAs will consider such international factors as cross-border infrastructure, international vulnerabilities, and global interdependencies in their SSPs.

Interagency Coordination – Review of Existing Mechanisms to Support the NIPP: The International Affairs offices in U.S. government agencies maintain existing relationships with foreign counterpart ministries and agencies, and are the primary partners with the Department of State in coordinating with foreign governments on international CI/KR matters.

DHS also works with SSAs to ensure that SSPs reflect international factors, such as cross-border infrastructure, international interdependencies, and global vulnerabilities.

The Department of State presently chairs an interagency working group that coordinates U.S. international CI/KR protection outreach activities. Within 30 days of publication of this Plan, the Department of State and DHS will review the working group's charter and its coordination mechanisms to ensure they address all international CI/KR issues specified by the NIPP. The Department of State and DHS will, within an additional 30 days, implement any changes that are needed to ensure that all NIPP requirements will be met and that the working group's charter reflects a role that best supports the comprehensive international CI/KR protection strategy.

1B.4.2 Foreign Aspects of International CI/KR Protection

International cooperation on cybersecurity and other CI/KR protection issues of a global nature is necessary because of the cross-border or borderless nature of these infrastructures. These efforts require interaction on both the policy and the operational levels and involve a broad range of entities from both the government and the private sector. Interaction on the international aspects of CI/KR protection takes place bilaterally, regionally, and multilaterally:

- **Bilateral:** DHS, in conjunction and consultation with the Department of State, participates in bilateral discussions and programs with countries of interest where issues are best addressed on a country-to-country basis.

- 1 • **Regional:** DHS and the Department of State partner together to provide leadership in regional groups,
2 such as the Organization of American States and the Asia Pacific Economic Cooperation, to raise
3 awareness and develop cooperative programs.
4 The United States engages with Canada and Mexico, as regional neighbors, on critical infrastructure
5 protection to enhance collaboration efforts. Current activities include the U.S., Canada, and Mexico
6 trilateral Security and Prosperity Partnership; the U.S.-Canada Critical Infrastructure Protection
7 Framework for Cooperation (Smart Border Action Plan); and the U.S.-Mexico Critical Infrastructure
8 Protection Framework for Cooperation (Border Partnership Action Plan).
9 • **Multilateral:** Multilateral collaboration on this aspect of CI/KR involves initiatives on the part of the
10 Organization for Economic Cooperation and Development (OECD), G8, and United Nations. For the
11 cybersecurity aspects of global CI/KR protection, DHS has established a preliminary framework for
12 cooperation on cybersecurity policy, watch and warning, and incident response for CI/KR with key allies
13 such as Australia, Canada, New Zealand, and the United Kingdom. DHS is coordinating and
14 participating in the establishment of an International Watch and Warning Network among cybersecurity
15 policy, computer emergency response, and law enforcement participants of 15 countries. The
16 International Watch and Warning Network will provide a mechanism for the participating countries to
17 share information to build cyber situational awareness and coordinate incident response.

18 1B.4.3 Working With Specific Countries and International Organizations

19 DHS, SSAs, and other security partners will work with other countries to promote CI/KR protection best
20 practices and they will pursue infrastructure security through international/multinational organizations such
21 as the G8, NATO, the European Union, the Organization of American States, the OECD, and Asia-Pacific
22 Economic Cooperation. The approach to working with some specific countries and organizations is founded
23 on formal agreements that address cooperation on CI/KR protection.

- 24 • **Canada and Mexico:** The CI/KR relationships between the United States and its immediate neighbors
25 make the borders virtually transparent. Electricity, natural gas, oil, telecommunications, roads, rail,
26 food, water, minerals, and finished products flow both ways across the borders. The importance of this
27 trade, and the infrastructures that support it, was highlighted after the terrorist attacks of September 11,
28 2001, nearly closed both borders. The United States entered into the 2001 Smart Border Declaration
29 with Canada and the 2002 Border Partnership Declaration with Mexico, in part, to address bilateral
30 CI/KR issues. In addition, the 2005 Security and Prosperity Partnership of North America (SPP)
31 established a trilateral approach to common security issues. The SPP is based on the principle that the
32 prosperity of all three nations is dependent on mutual security. The SPP complements, rather than
33 replaces, existing agreements.
- 34 • **United Kingdom:** The United Kingdom is a close ally with long experience in fighting terrorism and
35 protecting its CI/KR. The United Kingdom has developed law enforcement and intelligence systems,
36 and the protection of the commercial facilities sector. Like the United States, most of the critical
37 infrastructure in the United Kingdom is under private management. The government of the United
38 Kingdom has developed an effective, sophisticated system of managing public-private partnerships.
39 DHS has formed a Joint Contact Group with the United Kingdom that brings officials into regular, formal
40 contact to discuss and resolve a range of bilateral homeland security issues.

- 1 • **G8:** In the recent terrorist attacks against the United States, Spain, and the United Kingdom, the
2 infrastructures in G8 countries were exploited and used to inflict casualties and fear. The G8 has
3 underscored its determination to combat all forms of terrorism and to strengthen international
4 cooperation. Counterterrorism work has been the focus of a number of initiatives launched at recent
5 summits. At their meeting in Gleneagles Hotel in Scotland, in July 2005, the G8 heads of government
6 issued a Statement on Counter-Terrorism. In it, they pledged to “commit ourselves to new joint efforts.
7 We will work to improve the sharing of information on the movement of terrorists across international
8 borders, to assess and address the threat to the transportation infrastructure, and to promote best
9 practices for rail and metro security.” DHS will work closely with the G8 to address the common threats
10 to CI/KR and cyberspace.
- 11 • **European Union (EU):** The EU is pursuing CI/KR as a matter of policy, noting that an effective
12 strategy should focus on both preparedness and on consequence management. DHS will engage the
13 EU early in this process to share its experience, and to further cooperate on characteristics and
14 common vulnerabilities of critical infrastructure and cyberspace, risk analysis techniques, and
15 strategies to reduce risk and minimize consequences.
- 16 • **NATO:** NATO addresses CI/KR issues through the Senior Civil Emergency Planning Committee
17 (SCEPC), the senior policy and advisory body to the North Atlantic Council on civil emergency planning
18 and disaster relief matters. The Committee is responsible for policy direction and coordination of
19 Planning Boards and Committees in the NATO environment. It has developed considerable expertise
20 that applies to CI/KR protection and has planning boards and committees covering Ocean Shipping,
21 Inland Surface Transport, Civil Aviation, Food and Agriculture, Industrial Preparedness, Civil
22 Communications Planning, Civil Protection, and Civil-Military Medical Issues. DHS has a delegation to
23 SCEPC at NATO, participates in NATO’s telecommunications working group, and engages with NATO
24 in preparedness exercises.

25 1B.4.4 Foreign Investment in U.S. CI/KR

26 Infrastructure protection may be affected by foreign investment and ownership of sector assets. At the
27 Federal level, this issue is monitored by the Committee on Foreign Investment in the United States (CFIUS)
28 and, in some cases, the Federal Communications Commission (FCC). In February 2003, DHS was added
29 to the CFIUS. The council also includes the secretaries of State, Defense, and Commerce; the Attorney
30 General; the Director of the Office of Management and Budget; the U.S. Trade Representative; and the
31 Chairman of the Council of Economic Advisers, and is chaired by the Secretary of the Treasury.

32 DHS has important responsibilities on these government commissions that support the NIPP. These
33 include:

- 34 • As a member of the Committee on Foreign Investments, DHS performs an examination of the impact of
35 proposed foreign investments on CI/KR protection. The committee coordinates the development and
36 negotiation of security agreements with foreign entities that may be necessary to manage the risk to
37 CI/KR that a foreign investment may pose. DHS leads government monitoring activities aimed at
38 ensuring compliance with these agreements.

- DHS acts as a partner with the Department of Justice in supporting executive branch reviews of applications to the FCC from foreign entities pursuant to Section 214 of the Communications Act of 1934 to assess if they pose any threat to CI/KR protection.

1B.4.5 Information Sharing

Effective international cooperation of CI/KR protection requires a system for information sharing that includes processes and protocols for updates among all partners, mechanisms for systematic sharing of best practices, and frequent opportunities for partners to meet to discuss and address international CI/KR issues.

The Homeland Security Operations Center (HSOC) serves as the Nation's hub for information sharing and situational awareness for domestic incident management, increasing coordination among those members of the international community that are involved because of the role they play in protecting U.S. CI/KR.

The Homeland Security Information Network (HSIN) supports ongoing information-sharing efforts by offering Communities of Interest for selected international partners requiring close coordination with the HSOC.

DHS also provides mechanisms, such as the U.S. Computer Emergency Readiness Team (US-CERT) Portal, to improve information sharing and coordination among government communities and selected international security partners for cybersecurity. Additionally, the Cybercop Portal is a secure Internet-based information-sharing mechanism for law enforcement members involved in the field of electronic crimes investigations. This secure, Internet-based collaborative tool links and supports the law enforcement and investigative community worldwide, serving participants from more than 40 countries.

1B.5 Integration With Other Plans

The NIPP brings a new focus to international security cooperation and provides a risk-based strategic framework for measuring the effectiveness of international activities. The NIPP processes serve as management tools to assess international vulnerabilities and interdependencies. The NIPP process complements long-standing cooperative agreements with Canada, Mexico, the United Kingdom, NATO, and others, and provides the framework for collaborative engagement with additional international partners.

SSPs are required to include a description of sector relationships, as well as the roles and responsibilities of security partners, which include international/multinational organizations and foreign countries. They are also required to take a comprehensive, integrated view of the asset, including the characteristics, dependencies, and interdependencies; international links; and cyber systems needed for it to function.

1B.6 Ensuring International Cooperation Over the Long Term

The effort to ensure a sustainable approach to addressing the international aspects of CI/KR protection over the long term requires special consideration in the following areas:

- **Awareness:** Awareness of international aspects of CI/KR protection issues helps ensure implementation of effective, coordinated, and integrated CI/KR protection measures and helps enable

1 CI/KR security partners to make informed decisions. Often these issues are not apparent to those who
2 can take the most effective action because of the complexity of the international systems affecting
3 CI/KR protection. Awareness programs designed to identify such issues and provide the common
4 framework that allow these issues to be effectively addressed by security partners are required for
5 continued support for protection programs over the long term.

- 6 • **Training and Education:** NIPP training topics for managers and staff responsible for CI/KR that
7 require emphasis include international considerations for CI/KR protection because of the complex
8 considerations that often accompany international linkages and initiatives. Because training and
9 education programs can result in a higher quality workforce for international security partners, they
10 provide benefits over entire careers rather than on a one-time basis as direct aid to international
11 partners often does. Additionally, DHS will ensure that the organizational and sector expertise needed
12 to implement the international aspects of the NIPP program over the long term is developed and
13 maintained through exercises that include adequate testing of international CI/KR protection measures
14 and plans.
- 15 • **Research and Development:** Cooperative and coordinated research efforts are one of the most
16 effective ways to improve protective capabilities or to dramatically lower the costs of existing
17 capabilities so that international security partners can afford to do more with their limited budgets.
18 Techniques and designs developed through research can cost very little to share with international
19 security partners and, although the lead times needed for maturation of technology from the laboratory
20 to the field can be decades, such improvements can have wider applicability or much greater
21 effectiveness than available through current methods.
- 22 • **Plan Update:** NIPP and SSP updates proceed according to a specified schedule; however, the
23 international situation often changes in unpredictable ways and NIPP and SSP updates must be
24 coordinated as required with international agreements affecting CI/KR protection.

- 1 Appendix 2: Authorities, Roles and Responsibilities
- 2 Appendix 2A: Summary of Relevant Statutes, Strategies, and Directives
- 3 Appendix 2B: NIPP Implementation Initiatives and Actions

Appendix 2A: Summary of Relevant Statutes, Strategies, and Directives

This summary provides additional information on a variety of statutes, strategies, and directives referenced in Chapters 2 and 5, as applicable to CI/KR protection. This list is not inclusive of all authorities related to CI/KR protection; it includes the authorities most relevant to national-level, cross-sector CI/KR protection. Please note that there are many other authorities that are related to specific sectors.

2A.1 Statutes

Homeland Security Act of 2002 (November 2002)

This Act established a Cabinet-level department headed by a Secretary of Homeland Security with the mandate and legal authority to protect the American people from the continuing threat of terrorism. In the Act, Congress assigned DHS the primary missions to:

- Prevent terrorist attacks within the United States;
- Reduce the vulnerability of the United States to terrorism at home;
- Minimize the damage and assist in the recovery from terrorist attacks that occur; and
- Act as the focal point regarding natural disasters and malicious events, and emergency planning.

This statutory authority defined the protection of CI/KR as one of the primary missions of the Department and, combined with the President's direction in HSPD-7, mandated the unified, effective approach to CI/KR protection taken in the NIPP.

Intelligence Reform and Terrorism Prevention Act of 2004 (December 2004)

This Act established national standards for the issuance of identification documents, including drivers' licenses, social security cards, and birth certificates.

Federal Information Security Management Act (FISMA) (December 2002)

This Act required that Federal agencies develop a comprehensive information technology security program to ensure the effectiveness of information security controls over information resources that support Federal operations and assets. This legislation is relevant to the part of the NIPP that governs the protection of Federal assets and the implementation of cyber-protective measures under the Government Facilities SSP.

Federal Information Processing Standards (FIPS)

Federal Information Processing Standards are developed by the National Institute of Standards and Technology only when there are no existing voluntary standards to address the Federal requirements for the interoperability of different systems, the portability of data and software, and computer security.

Gramm-Leach-Bliley Act (1999)

This Act provides limited privacy protections against the sale of private financial information. The Act codifies protections against the practice of obtaining personal information through false pretenses. The Act provides for the privacy and protection of information that may be collected under the auspices of the NIPP.

The Defense Production Act of 1950 and the Defense Production Reauthorization Act of 2003 (December 2003)

This Act provides the primary authority to ensure the timely availability of resources for national defense and civil emergency preparedness and response. Among other powers, this Act authorizes the President to demand that companies accept and give priority to government contracts that the President “deems necessary or appropriate to promote the national defense,” and allocate materials, services, and facilities, as necessary, to promote the national defense in a major national emergency. This Act also authorizes loan guarantees, direct loans, direct purchases, and purchase guarantees for those goods necessary for national defense. It also allows the President to void international mergers that would adversely affect national security. This Act defines “national defense” to include critical infrastructure protection and restoration, as well as activities authorized by the emergency preparedness sections of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (October 2000). Consequently, the authorities stemming from this Act are available for activities and measures undertaken in preparation for, during, or following a natural disaster or accidental or malicious event. The Department of Commerce has redelegated these authorities under Executive Order 12919, National Defense Industrial Resource Preparedness, June 7, 1994, as amended, to the Secretary of Homeland Security to place and, upon application, to authorize State and local governments to place priority-rated contracts in support of Federal, State, and local emergency preparedness activities. The Act has a national security nexus with the NIPP. National emergencies related to CI/KR may arise that require the President to use his authority under the Act.

Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (June 2002)

This Act improves the ability of the United States to prevent, prepare for, and respond to bioterrorism and other public health emergencies. Key provisions of the Act, 42 U.S.C. §§ 247d and 300hh among others, address: (1) development of a national preparedness plan by the Department of Health and Human Services that is designed to provide effective assistance to State and local governments in the event of bioterrorism or other public health emergencies; (2) operation of the National Disaster Medical System to mobilize and address public health emergencies; (3) grant programs for the education and training of public health professionals and the improvement of State, local, and hospital preparedness for, and response to, bioterrorism and other public health emergencies; (4) streamlining and clarification of communicable disease quarantine provisions; (5) enhancement of controls on dangerous biological agents and toxins; and (6) protection of the safety and security of food and drug supplies.

Cybersecurity Research and Development Act (November 2002)

This Act allocates funding to the National Institute of Standards and Technology and the National Science Foundation for the purposes of facilitating increased R&D for computer network security and supporting

research fellowships and training. The Act establishes a means of enhancing basic R&D related to improving the cybersecurity of CI/KR.

Critical Infrastructure Information (CII) Act of 2002

This Act created a framework that enables members of the private sector to voluntarily submit sensitive information regarding the Nation's critical infrastructure to DHS with the assurance that the information, if it satisfies certain requirements, will be protected from public disclosure.

The Protected Critical Infrastructure Information (PCII) Program, created by the Act, is central to the information-sharing and protection strategy of the NIPP. By protecting sensitive information submitted through the Program, the private sector is assured that the information will remain secure and only be used to further CI/KR protection efforts.

USA PATRIOT Act of 2001

This Act outlined the domestic policy related to deterring and punishing terrorists, and the U.S. policy for critical infrastructure protection. It also seeks to establish a national competence for critical infrastructure protection. The Act established the National Infrastructure Simulation and Analysis Center (NISAC) and outlined the U.S. government's commitment to understanding and protecting the interdependencies among critical infrastructures.

2A.2 National Strategies

The National Strategy for Homeland Security

This Strategy established the Nation's strategic homeland security objectives and outlined the six critical mission areas necessary to achieve those objectives. The Strategy also provided a framework to align the resources of the Federal budget directly to the task of securing the homeland. The Strategy specified eight major initiatives to protect the Nation's CI/KR, one of which specifically called for the development of the NIPP.

National Strategy for the Physical Protection of Critical Infrastructures and Key Assets

This Strategy identified the policy, goals, objectives, and principles for actions needed to "secure the infrastructures and assets vital to national security, governance, public health and safety, economy and public confidence." The Strategy provided a unifying organizational structure for CI/KR protection and identified specific initiatives related to the NIPP to drive near-term national protection priorities and inform the resource allocation process.

National Strategy to Secure Cyberspace

This Strategy set forth objectives and specific actions to prevent cyber attacks against America's CI/KR, reduce nationally identified vulnerabilities to cyber attacks, and minimize damage and recovery time from

cyber attacks. The Strategy provided the vision for cybersecurity and served as the foundation for the protection of the cyber component of CI/KR.

2A.3 Homeland Security Presidential Directives

HSPD-1: Organization and Operation of the Homeland Security Council (October 2001)

HSPD-1 established the Homeland Security Council (HSC) and a committee structure for developing, coordinating, and vetting homeland security policy among executive departments and agencies. The Directive provided a mandate for the HSC to ensure the coordination of all homeland security-related activities among executive departments and agencies and promoted the effective development and implementation of all homeland security policies. The HSC is responsible for arbitrating and coordinating any issues that may arise among the different departments and agencies under the NIPP.

HSPD-2: Combating Terrorism Through Immigration Policies (October 2001)

HSPD-2 established policies and programs to enhance the Federal government's capabilities for preventing aliens who engage in or support terrorist activities from entering the country, and for detaining, prosecuting, or deporting any such aliens who are in the United States.

HSPD-2 also directed the Attorney General to create the Foreign Terrorist Tracking Task Force to ensure that, to the maximum extent permitted by law, Federal agencies would coordinate programs to accomplish the following: (1) deny entry into the United States of aliens associated with, suspected of being engaged in, or supporting terrorist activity; and (2) locate, detain, prosecute, or deport any such aliens already present in the United States.

HSPD-3: Homeland Security Advisory System (HSAS) (March 2002)

HSPD-3 mandated the creation of an alert system for disseminating information regarding the risk of terrorist acts to Federal, State, and local authorities, and the public. It also included a corresponding set of protective measures for Federal, State, and local governments to implement, depending on the threat condition. This Directive established policy for the creation of an HSAS, which provides a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to Federal, State, and local authorities, and to the American people. Such a system provides warnings in the form of a set of graduated "Threat Conditions" that are elevated as the risk of the threat increases. At each Threat Condition, Federal departments and agencies are required to implement a corresponding set of "protective measures" and increase the steady-state protection measures.

HSPD-4: National Strategy to Combat Weapons of Mass Destruction (WMD) (December 2002)

HSPD-4 set forth this Strategy, which is based on three principal pillars: (1) Counter-Proliferation to Combat WMD Use, (2) Strengthened Nonproliferation to Combat WMD Proliferation, and (3) Consequence Management to Respond to WMD Use. This Directive outlined four cross-cutting functions that needed to be pursued on a priority basis: (1) intelligence collection and analysis on WMD, delivery systems, and

related technologies; (2) R&D to improve our ability to address evolving threats; (3) bilateral and multilateral cooperation; and (4) targeted strategies against hostile nations and terrorists.

HSPD-5: Management of Domestic Incidents (February 2003)

HSPD-5 established a national approach to domestic incident management that ensures effective coordination among all levels of government, and between the government and the private sector. Central to this approach are the National Incident Management System (NIMS) – an organizational framework for all levels of government, and the NRP – an operational framework for incident response at the Federal level.

In this Directive, the President designated the Secretary of Homeland Security as the principal Federal official for domestic incident management and empowered the Secretary to coordinate Federal resources used for prevention, preparedness, response, and recovery related to terrorist attacks, major disasters, or other emergencies in specific cases. The Directive assigned specific responsibilities to the Attorney General, Secretary of Defense, Secretary of State, and the Assistants to the President for Homeland Security and National Security Affairs, and directed the heads of all Federal departments and agencies to provide their “full and prompt cooperation, resources, and support,” as appropriate and consistent with their own responsibilities for protecting national security, to the Secretary of Homeland Security, Attorney General, Secretary of Defense, and Secretary of State in the exercise of leadership responsibilities and missions assigned in HSPD-5. The Directive also noted that it does not alter, or impede the ability to carry out, the authorities of Federal departments and agencies to perform their responsibilities under law.

HSPD-6: Integration and Use of Screening Information (September 2003)

HSPD-6 consolidated the Federal government's approach to terrorist screening by establishing a Terrorist Screening Center (TSC). Federal departments and agencies are directed to provide terrorist information to the Terrorist Threat Integration Center (TTIC), which is then required to provide all relevant information and intelligence to TSC. In order to protect against terrorism, this Directive established the national policy to: (1) develop, integrate, and maintain thorough, accurate, and current information about individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism (Terrorist Information); and (2) use that information, as appropriate and to the full extent permitted by law, to support (a) Federal, State, Territorial, local, tribal, foreign government, and private sector screening processes; and (b) diplomatic, military, intelligence, law enforcement, immigration, visa, and protective processes.

HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection (December 2003)

HSPD-7 established a framework for Federal departments and agencies to identify, prioritize, and protect CI/KR from terrorist attacks, with an emphasis on protecting against catastrophic health effects and mass casualties. This Directive established a national policy for Federal departments and agencies to identify and prioritize U.S. CI/KR and to protect them from terrorist attacks. HSPD-7 mandated the creation and implementation of the NIPP and set forth roles and responsibilities for DHS; SSAs; other Federal departments and agencies; and State, local, tribal, private sector, and other security partners.

HSPD-8: National Preparedness (December 2003)

HSPD-8 established policies to strengthen the preparedness of the United States to prevent, protect, respond to, and recover from threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal; establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments; and outlining actions to strengthen the preparedness capabilities of Federal, State, and local entities. This Directive mandated development of the goal to guide emergency preparedness training, planning, equipment, and exercises, and to ensure that all adhere to the same standards. The Directive established an inventory of Federal response capabilities and refined the process by which preparedness grants are administered, disbursed, and utilized at the State and local levels.

HSPD-9: Defense of United States Agriculture and Food (January 2004)

HSPD-9 established an integrated national policy for improving intelligence operations, emergency response capabilities, information-sharing mechanisms, mitigation strategies, and sector vulnerability assessments to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies.

HSPD-10: Biodefense for the 21st Century (April 2004)

HSPD-10 integrated the biodefense programs and initiatives of the national and homeland security, medical, public health, intelligence, diplomatic, and law enforcement communities into a comprehensive national program to address threats from biological weapons. This Directive provided a comprehensive framework for the Nation's biodefense and, among other actions, delineated the roles and responsibilities of Federal agencies and departments in continuing their work in this area.

HSPD-11: Comprehensive Terrorist-Related Screening Procedures (August 2004)

HSPD-11 required the creation of a strategy and implementation plan for a coordinated and comprehensive approach to terrorist screening in order to improve and expand procedures to screen people, cargo, conveyances, and other entities and objects that pose a threat.

HSPD-12: Policy for a Common Identification for Federal Employees and Contractors (August 2004)

HSPD-12 established a mandatory, government-wide standard for secure and reliable forms of identification issued by the Federal government to its employees and contractors in order to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy.

HSPD-13: Maritime Security Policy (December 2004)

HSPD-13 directs the coordination of U.S. government maritime security programs and initiatives to achieve a comprehensive and cohesive national effort involving the appropriate Federal, State, local, and private sector entities. The Directive also established a Maritime Security Policy Coordinating Committee to coordinate interagency maritime security policy efforts.

HSPD-14: Domestic Nuclear Detection (April 2005)

HSPD-14 established the effective integration of nuclear and radiological detection capabilities across Federal, State, local, and tribal governments and the private sector for a managed, coordinated response. This Directive supports and enhances the effective sharing and use of appropriate information generated by the intelligence community, law enforcement agencies, counterterrorism community, other government agencies, and foreign governments, as well as providing appropriate information to these entities.

2A.4 Other

Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, as Amended by Executive Order 13286

This Executive Order established the National Communications System (NCS) as a Federal interagency group that is assigned national security and emergency preparedness (NSEP) telecommunications responsibilities throughout the full spectrum of emergencies. The NSEP objective is to ensure that the Federal government has telecommunications services that will function under all conditions, including emergency situations. Under the policy objectives stated in Executive Order 12472 and National Security Decision Directive 97, these responsibilities include planning for, developing, and implementing enhancements to the national telecommunications infrastructure to achieve measurable improvements in survivability, interoperability, and operational effectiveness under all conditions, and seeking greater effectiveness in managing and using national telecommunications resources to support the government during any emergency. The NCS regularly interacts with public managers involved in cross-sector telecommunications issues and serves as the primary support for the National Security Telecommunications Advisory Committee (NSTAC). In addition to its cross-sector role, NCS is the DHS-designated SSA for the Telecommunications Sector.

Executive Order 13130, National Infrastructure Assurance Council (NIAC)

This Executive Order established the NIAC as an effort by both government and private sector entities to address threats to our Nation's CI/KR.

The NIAC is an important complement to the NIPP and serves as an important resource since NIAC members represent the vast majority of private sector infrastructure owners and operators.

1 Appendix 2B: NIPP Implementation Initiatives and Actions

Notes: X = Required action O = Recommended or encouraged action

Chapter and Section		Milestone				Security Partner					
		90 Days After NIPP Approval	180 Days	365 Days	Specific Date	DHS	Sector-Specific Agency	Other Federal	State or Territory	Local and Tribal	Private Sector
2	AUTHORITIES, ROLES, AND RESPONSIBILITIES										
	Complete SSP development.		+			X					
	Submit Annual CI/KR Protection Reports to DHS.				Jul 1	X	X	X	O	O	
	Complete National NIPP Funding Report.				Sep 1	X					
	Review and revise CI/KR-related plans as needed to align them with the NIPP.		+			X	X	X			
	Review and revise homeland security program and associated plans as needed to align them with the NIPP.			+					O	O	O
3	THE PROTECTION PROGRAM STRATEGY: REDUCING RISK										
3.1	Set Security Goals										
	Develop and update the national risk profile in collaboration with security partners.			+		X					
	Establish sector security goals that support NIPP goals and objectives.		+				X				
3.2	Identify Assets										
	Identify desired information by asset type and develop sector inventory guidance.	+				X	X	X	O	O	O
	Develop tools and methodologies to assist security partners in identifying cyber assets.		+			X					
3.3	Assess Risks										
3.3.1	Baseline Criteria for Assessment Methodologies										
	Review existing risk assessments or methodologies used to assess compatibility with the DHS baseline criteria. "Translate" the results or adjust the methodology if they differ from the baseline criteria.		+			X	X				
	Assist the SSAs and other security partners to determine the common criteria for risk assessments.		+			X					
3.3.2	Consequence Analysis										
	Provide a timeline for the development of sector-specific methodologies including RAMCAP modules and for conducting consequence-based top screening for all CI/KR sectors.	+				X	X				
	Define common terminology and metrics for use in assessing consequences.		+			X					
	Conduct consequence-based top screening for first priority CI/KR sectors.		+			X	X		O	O	O
	Work with security partners to develop consequence assessment methodologies for the first priority CI/KR sectors with completed top screening.		+			X	X				
	Conduct consequence assessments at CI/KR assets with potentially high consequences for the first priority CI/KR sectors based on the results of the top-screening process.		+			X	X		O	O	O

Notes: X = Required action O = Recommended or encouraged action

Chapter and Section		Milestone				Security Partner					
		90 Days After NIPP Approval	180 Days	365 Days	Specific Date	DHS	Sector-Specific Agency	Other Federal	State or Territory	Local and Tribal	Private Sector
3.3.3	Vulnerability Assessment										
	Work with DHS to validate the results of assessments for sector assets that are of the greatest concern and involve owners and operators in the review whenever possible.	+					X			O	O
	Develop sector-specific vulnerability assessment methodologies (e.g. RAMCAP Vulnerability Assessment modules) for the first priority CI/KR sectors.		+			X	X				
	Conduct vulnerability assessments for CI/KR assets in the first priority sectors and identify common cross-sectors vulnerabilities.		+			X	X		O	O	O
3.3.4	Threat Analysis										
	Develop first quarterly sector-specific CI/KR threat assessment.	+				X					
	Identify intelligence collection requirements.			+		X		X			
3.4	Prioritize										
	Use analysis-based normalization tools to convert risk assessment results (analyses that do not meet the NIPP baseline criteria) into measures that can be used for national-level comparison.		+			X			O		
	Prioritize CI/KR protection needs based on normalized scores from risk assessments.		+			X			O		
3.5	Implement Protective Programs										
	Identify gaps in protection for high priority CI/KR.				Jul 1	X	X		O		
	Review current protective programs in relationship to identified gaps.				Jul 1	X	X		O		
	Augment existing programs, or design and implement new protective programs for the remaining gaps.				Sep 1	X	X		O	O	
3.6	Measure Effectiveness										
3.6.1	NIPP Metrics and Measures										
	Provide guidance on metrics for annual reporting and national-level, cross-sector comparative analysis.		+			X					
3.6.2	Gathering Performance Information										
	Gather information needed to measure performance associated with each set of core and sector-specific metrics.			+		X					
3.6.3	Assessing Performance and Reporting on Progress										
	Use risk assessment information to develop Annual Reports to the Secretary of Homeland Security.				Jul 1		X				
	Use risk assessment to inform Annual Reports to DHS on State CI/KR protection program.				Jul 1				O		
3.7	Continuous Improvement										
	Use national-level risk assessment to generate a cross-sector report that describes national progress toward CI/KR protection goals and needed improvements.				Sep 1	X					

Notes: X = Required action O = Recommended or encouraged action

Chapter and Section		Milestone				Security Partner					
		90 Days After NIPP Approval	180 Days	365 Days	Specific Date	DHS	Sector-Specific Agency	Other Federal	State or Territory	Local and Tribal	Private Sector
4	ORGANIZING AND PARTNERING FOR CI/KR PROTECTION										
4.1	Leadership and Coordination Mechanisms										
	Commence SSC and GCC operations.	+				X	X		O	O	O
	Establish a point of contact within DHS for national-level NIPP coordination with regional entities.	+				X					
	Implement mechanisms to enable selected regional entities to access the sector partnership model at the national level.		+			X	X				
	Review established coordination mechanisms to ensure that they accommodate NIPP requirements.			+					O	O	O
4.2	The Information-Sharing Strategy: A Networked Approach										
	<i>The Homeland Security Information Network</i>										
	Implement sector-specific policies and protocols for vetting and disseminating routine information to owners and operators.	+				X	X				
	Complete rollout of HSIN-CS to all sectors.			+		X					
	Work with security partners to measure the efficacy of the HSIN and identify requirements for new mechanisms or supporting technologies.			+		X	X	X	O	O	O
	<i>Lessons Learned and Best Practices</i>										
	Ensure that the NIMS Integration Center includes information on CI/KR protection best practices.	+				X	X				
4.3	Protection of Sensitive CI/KR Information										
	Review information protection practices to ensure they comply with the Interim PCII Rule and the Final Rule when published.		+			X					
5	INTEGRATING CI/KR PROTECTION AS PART OF THE HOMELAND SECURITY MISSION										
5.3	Relationship of the NIPP to Other CI/KR Protection Plans and Programs										
5.3.1	Sector-Specific Plans										
	Coordinate SSP planning with security partners, including completion of a review and concurrence process.		+				X				
	Review NIPP Base Plan and establish program management processes needed to support plan implementation within each sector.	+					X				
	Coordinate with the SSAs to provide guidance and support for SSP development.		+			X					
	Review SSPs to verify that cross-sector requirements have been identified.			+		X					
5.3.2	State, Regional, Local, and Tribal CI/KR Protection Programs										
	Review, revise, or develop homeland security program and associated plans as needed to ensure seamless linkage between the NIPP steady-state CI/KR protection and incident management activities.			+					O	O	
5.3.3	Other Security Partner Plans or Programs Related to CI/KR Protection										
	Review and revise CI/KR-related plans as needed to ensure seamless linkage between the NIPP steady-state		+			X	X	X			

Notes: X = Required action O = Recommended or encouraged action

Chapter and Section		Milestone				Security Partner					
		90 Days After NIPP Approval	180 Days	365 Days	Specific Date	DHS	Sector-Specific Agency	Other Federal	State or Territory	Local and Tribal	Private Sector
	CI/KR protection and incident management activities.										
	Review and revise homeland security program and associated plans as needed to ensure seamless linkage between the NIPP steady-state CI/KR protection and incident management activities.			+					O	O	O
5.4	CI/KR Protection and Incident Management										
	Review current Federal CI/KR protection measures to ensure alignment with the HSAS threat levels.		+			X	X	X			
	Review current State, local, tribal, and private sector CI/KR protection measures to ensure that they align with the HSAS threat levels.			+					O	O	O
	Develop written procedures to ensure seamless transition from steady-state CI/KR protection to activities required to inform and enable incident management decisions and activities.			+			X	X	O	O	O
6	ENSURING AN EFFECTIVE, EFFICIENT PROGRAM OVER THE LONG TERM										
6.1	Building National Awareness										
	Identify and assess the requirements for a national CI/KR protection awareness program.	+				X					
	Convene an interagency national CI/KR public awareness workgroup.	+				X					
	Conduct an inventory of existing national public awareness efforts or partnerships that could support the delivery of CI/KR protection messages to broad audiences.		+			X					
	Develop and implement a comprehensive national CI/KR protection awareness program.			+		X	X	X	O	O	O
	Conduct initial CI/KR protection public awareness activities called for under the national awareness plan within the State, local, and tribal jurisdictions.			+					O	O	
6.2	Enabling Education, Training, and Exercise Programs										
6.2.2	Education and Training										
	Review training programs to ensure that they are consistent with NIPP requirements.	+				X	X	X	O	O	O
	Provide the initial training on the NIPP to introduce all security partners to the Plan's contents and requirements.		+			X					
	Make recommendations for training program revision to conform to NIPP requirements.		+			X	X	X	O	O	O
	Revise training programs to conform to NIPP requirements.			+		X	X	X	O	O	O
6.2.3	Organizational Training and Exercise Programs										
	Ensure that DHS exercises include adequate testing of steady-state CI/KR protection measures and plans.			+		X					
	Ensure that DHS exercises include tests of the interaction between the NIPP framework and the NRP incident management framework.			+		X					
	Ensure that DHS exercises include a focus on CI/KR interdependencies and protection collaboration across			+		X					

Notes: X = Required action O = Recommended or encouraged action

Chapter and Section		Milestone				Security Partner					
		90 Days After NIPP Approval	180 Days	365 Days	Specific Date	DHS	Sector-Specific Agency	Other Federal	State or Territory	Local and Tribal	Private Sector
	jurisdictional and sector boundaries.										
6.3	Conducting Research and Development										
	Gather information on industry advances in CI/KR protection-related science and technology; ensure that these are periodically reviewed by the NSTC.		+			X	X	X			O
	Convene discussions and workshops with security partners to determine CI/KR R&D priorities.		+			X			O	O	O
	Share sector-specific threat handbooks with the CI/KR R&D communities to guide emphasis and timing of future R&D activities.		+			X	X	X			
	Identify and communicate to DHS requirements for CI/KR-related R&D for use in the national R&D planning effort.			+		X	X	X	O	O	O
	Develop a comprehensive database to manage Federal R&D investments related to CI/KR protection.			+		X	X	X			
	Work with OSTP to establish an updating cycle for the annual NCIP R&D Plan; update plan according to cycle.			+		X					
	Work with OSTP to incorporate sector-level R&D requirements into the updating of the NCIP R&D Plan.			+		X					
6.4	Building and Maintaining Databases, Simulations, and Other Tools										
6.4.1	National CI/KR Protection Data Systems										
	Establish appropriate data-collection formats for national infrastructure inventory.		+			X					
	Identify all databases containing information useful to CI/KR protection and national inventory.			+		X	X	X			
6.4.2	Simulation and Modeling										
	Establish requirements for the development, maintenance, and use of research- and operations-related modeling capabilities for CI/KR protection.		+			X					
	Review existing private sector modeling initiatives and opportunities for joint ventures to ensure that DHS and its security partners make maximum use of private sector modeling capabilities.			+		X					O
	Review existing SSA modeling capabilities for potential use in CI/KR protection.			+		X	X				
6.4.3	Coordination With Security Partners on Databases and Modeling										
	Specify the timelines and milestones for the initial population of asset databases.	+				X					
	Specify a regular schedule for maintenance and updating of databases.	+				X					
	Identify databases and other data services that can be used to populate asset databases.			+		X	X	X	O	O	O
	Outline sector plans and processes for the development and updating of databases, data systems, modeling, and simulation.			+			X				
6.5	Continuously Improving the NIPP and SSPs										
	Establish the mechanism(s) necessary to coordinate SSP review and maintenance.		+				X				

Notes: X = Required action O = Recommended or encouraged action

Chapter and Section		Milestone				Security Partner					
		90 Days After NIPP Approval	180 Days	365 Days	Specific Date	DHS	Sector-Specific Agency	Other Federal	State or Territory	Local and Tribal	Private Sector
	Conduct first annual review of the NIPP and SSPs to identify changes that warrant the issuance of a periodic update (e.g., new laws, orders, procedures, etc.).			+		X					
7	PROVIDING RESOURCES FOR THE CI/KR PROTECTION PROGRAM										
7.1	The Risk-Based Resource Allocation Process										
	Work with SSAs and the States to develop a national cross-sector picture of funding sources for CI/KR protection.	+				X	X	X	O		
	Work with the SSAs and the States to address funding gaps or duplicative efforts identified through the budget coordination.				Jul 1	X	X		O		
	Use information gathered from the SSAs and the States to assess cross-sector CI/KR protection efforts, progress, funding, and outstanding needs as the basis for the NIPP National Funding Report.				Sep 1	X	X		O		
	Work with respective department or agency budget process to identify and develop NIPP-related aspects of their annual budget submissions.				Sep 1	X	X	X	O	O	
7.2	Federal Resource Allocation Process for DHS, SSAs, and Other Federal Agencies										
	Coordinate Annual Report development with sector security partners, SCCs and GCCs to identify existing sector-specific CI/KR protection programs, NIPP-related initiatives, priorities, R&D funding and S&T investment requirements, critical gaps, and funding projections.				Jul 1	X	X	X	O	O	
	Develop and submit to OMB the National NIPP Funding Report that summarizes NIPP-related investment recommendations, identifies NIPP requirements, and summarizes NIPP funding requests across sectors and States.				Sep 1	X					
7.3	Federal Resources for State and Local Government Preparedness										
	Ensure annual homeland security grant guidance includes adequate consideration of CI/KR protection priorities.	+				X					
	Identify potential funding sources for State CI/KR protection efforts.		+				X				
	Develop guidance for State, Territorial, and tribal CI/KR protection programs to ensure they are aligned with grant application requirements.				as req	X					
	Work through the State Administrative Agencies to identify and prioritize the homeland security needs identified in State Homeland Security Strategies and Program and Capability Enhancement Plans, and identify assistance from all funding sources that may address these needs.				as req	X			O		
	Apply for homeland security grants to address CI/KR protection efforts per DHS/G&T guidance.				as req				O	O	

- 1 Appendix 3: The Protection Program
- 2 Appendix 3A: NIPP Baseline Criteria for Assessment Methodologies
- 3 Appendix 3B: Existing Protective Programs and Other In-Place Measures
- 4 Appendix 3C: National Asset Database

Appendix 3A: NIPP Baseline Criteria for Assessment Methodologies

The purpose of this appendix is to specify the baseline criteria for methodologies used to support national comparative risk analysis under the NIPP framework.

Many owners and operators have performed vulnerability and/or risk assessments on the assets, systems, and networks under their control. To take advantage of these previous activities, DHS plans to use the results from previously performed assessments wherever possible. However, the assessment work to date has varied widely both within and across sectors in terms of its comprehensiveness, objectivity, inclusion of threat and consequence considerations, physical and cyber dependencies, and other characteristics. In order to use previous assessment results to support national comparative risk analysis, the methodologies used to perform the assessments must be tested against the NIPP Baseline Criteria.

3A.1 Baseline Criteria

There are seven criteria constitute the national baseline, categorized generally into two different groups. The first group tests the methodology to ensure that it will be *credible* to objective users of the analysis produced by methodology; the second group tests the methodology to ensure that it will be *comparable* with other standard methods used in comparative sector or national risk assessment.

To be credible, a methodology must have a sound basis (it must have integrity); it also must be complete and defensible; these factors are reflected in the first three elements of the criteria. To be comparable, the methodology must be documented, transparent, reproducible, and accurate; these factors are reflected in the last four elements of the criteria.

The following questions provide a simple way to determine which aspects of a methodology meet the baseline criteria. The questions also provide a guide for improving the methodologies or changing them so that they can meet the baseline criteria. A methodology meets the requirements of the baseline criteria when all of the questions are answered in the affirmative.

Is the Methodology Credible?

1. **Integrity (sound basis):** Is the methodology based on classic risk analysis and security vulnerability analysis? Does it specifically address:
 - a. Consequences?
 - b. Vulnerability?
 - c. Threat?
2. **Complete:** Does the methodology provide reasonably complete results via a quantitative, systematic, and rigorous process that:
 - a. Provides numerical values for estimated *consequences*, *vulnerability*, and *threat* whenever possible, or uses scales when numerical values are not possible?
 - b. Specifically addresses both health and direct economic *consequences*?

c. Considers existing protective measures and their effects on *vulnerabilities* as a baseline?

d. Examines physical, cyber, and human *vulnerabilities*?

e. Applies the worst-reasonable-case standard when assessing *consequences* and choosing *threat* scenarios?

f. Uses *threat*-based *vulnerability* assessments?

3. **Defensible:** Is the methodology thorough and does it use the recognized methods of the professional disciplines relevant to the analysis? Does it adequately address the relevant concerns of governments, employees, and the public?

Is the Methodology Comparable to Other Methodologies?

1. **Documented:** Does the methodology provide clear and sufficient documentation of the analysis process and the products that result from its use?

2. **Transparent:** Is the methodology easily understandable to others as to:

a. Assumptions used?

b. Key definitions?

c. Units of measurement?

d. How it is to be accomplished?

e. Basis for expert judgments and risk decisions?

3. **Reproducible:** Does the methodology provide results that are reproducible or verifiable by equivalently experienced or knowledgeable personnel?

4. **Accurate:** Is the methodology free from obvious errors or omissions so that the results are suitable to inform decision making?

Given the unique nature of the individual CI/KR sectors and the assets, systems, and networks that comprise them, details of the baseline criteria must be tailored to each sector. DHS will work with sector security partners to accomplish this tailoring; however, the baseline criteria above are generally applicable to each sector.

Existing assessments or methodologies will be accepted by DHS as meeting the NIPP Baseline Criteria if they can provide an adequate response to the questions above.

3A.2 Specific Aspects of the NIPP Baseline Criteria

Based on classical risk analysis. As outlined in Chapter 3 of the NIPP, risk analysis consists of consequence, vulnerability, and threat analyses. To be considered credible, a proposed methodology must include all three components of risk assessment.

Provide numerical values when possible; use scales when necessary. Risk typically can be measured either quantitatively (i.e., numerically) or qualitatively (i.e., descriptively). Health and economic impacts generally lend themselves to quantitative measurement (e.g., number of lives lost, cost in dollars of

rebuilding an asset), whereas psychological and governance impacts are often measured qualitatively. For quantitatively measured consequences and their associated risk, precise numerical estimates should be used whenever possible. When it is not practical to use precise estimates, scales should be used to reflect the assessed outcome using either numerical ranges (for quantitative metrics) or detailed descriptions (for qualitative metrics). The use of numerical ranges and/or detailed descriptions is necessary because terms such as “low” or “high” are subject to varied interpretation by different users. DHS will provide sample ranges and descriptive language to security partners, and will work with security partners to establish “translators” that facilitate the conversion of results using other methodologies to standard scales to support national comparative risk analysis.

Consider health and direct economic consequences. For the national comparative risk analysis conducted by DHS, the consequences of interest are those of national significance as established in HSPD-7. These consequences can be divided into four main categories: health, economic, psychological, and governance impacts. Because accurately estimating indirect economic, psychological, and governance impacts is difficult and often beyond the scope of an individual asset owner’s expertise, this element of the baseline criteria requires assessment methodologies to address the following two types of impact as a minimum:

1. **Health Impact:** Effect on human life and physical well-being (e.g., fatalities, injuries).
2. **Economic Impact:** Direct and indirect effects on the national, State, tribal, or local economy (e.g., cost to rebuild asset, cost to respond to and recover from attack, or other incident downstream costs resulting from unavailability of product or service).

Consider existing protective measures and their impacts as the baseline. In evaluating the extent to which an asset is vulnerable or an attack is likely, an assessment should consider the existing measures that are in place to reduce that asset’s exposure to the relevant threat scenarios. Specifically, security specialists should examine the ability of an asset’s existing security profile to deter, detect, devalue, defend against, mitigate, respond to, and recover from the most relevant threat scenarios.

Use worst-reasonable-case standard. Risk assessments are significantly influenced by the estimated or assumed level of success or severity of a given threat scenario (e.g., worst case, worst reasonable case, most likely). For the purposes of national comparative risk assessment, methodologies should use a worst-reasonable-case scenario.

Examine physical, cyber, and human vulnerabilities. When evaluating risk, many vulnerability assessments focus solely on physical security; however, physical security is only one aspect of a robust vulnerability assessment. Vulnerability assessments should also assess personnel security and other human security issues, cybersecurity and network architecture issues, operational security, and infrastructure dependencies and interdependencies.

Scenario-based vulnerability assessments. The suite of tools that DHS is developing and using for vulnerability assessments is scenario based, meaning that the assessments measure the susceptibility of an identified asset or system to a specific threat scenario (e.g., successful detonation of a nuclear bomb at the asset, successful detonation of a car bomb at the asset). This allows the assessment to be informed in general terms by potential adversary tactics and weapons. Consequently, vulnerability assessment methodologies used to support DHS cross-sector comparative risk analyses should be scenario based, and

certain specific scenarios or their equivalent should be used. In light of the distinct characteristics associated with different types of assets, systems, or networks, DHS will work with sector partners to identify which threat scenarios are most appropriate in the context of the sector-specific landscape.

Defensible on logical grounds. In order to produce analysis that is credible to those who must use its results, a methodology must adhere to the recognized methods of the professional disciplines that are relevant to the analysis (e.g., economics, engineering, medical profession), and it must reasonably and adequately address the concerns raised by the three groups who may be directly affected by the decisions based on its results: (1) governments at all levels, (2) employees, and (3) the public at large (which can include other stakeholders, such as dependent infrastructure sectors).

Documentation is necessary to enable comparison with other methodologies in use. Written documentation that is clear and sufficiently complete to allow a comparison of strengths and weaknesses with respect to other methodologies used in the national comparative risk assessment is necessary. This should include a description of assumptions, definitions, units of measurement, time horizon, the general order and steps of the assessment, calculations, and the basis for any expert judgments that the methodology relies on that are not readily apparent.

Need to be easily understandable. In addition to the existence of written documentation, a methodology must be easily understandable to others with appropriate knowledge and experience. This means that:

- Assumptions must be stated;
- Key definitions must be provided;
- Units of measurement must be specified;
- Analytic process by which the methodology is executed should be provided; and
- Basis for expert judgments used in lieu of explicit calculations or analysis should be provided.

As with any deliberate process, the results of applying the methodology must be reproducible or verifiable by others of requisite knowledge and experience. The methodology must be sufficiently defined and deliberate so that any qualified person could replicate the results it produces; it must not depend on hidden judgments or opinions.

Must be free from logical errors of omission or commission. Because the results of risk assessments will be used to inform decisions regarding homeland security, the accuracy of the methodology must meet a high standard. While estimates and approximations often must be used, the tradeoff between practicality and exactness must be carefully taken into account, and, in no case, should logical or mathematical errors be accepted.

Appendix 3B: Existing Protective Programs and Other In-Place Measures

This appendix provides examples of the protective programs that currently support NIPP implementation. The examples provided here generally cut across sectors and have national significance. The SSPs address sector-specific programs that are conducted under the leadership of the SSAs.

3B.1 Protective Programs and Initiatives

Buffer Zone Protection Program (BZPP): The BZPP is a grant program designed to provide resources to State, Territorial, and local law enforcement and other security professionals to enhance security “outside the fence” of CI/KR facilities, thereby making it more difficult for terrorists to conduct surveillance or successfully launch an attack from the immediate vicinity of a potential target.

Comprehensive Reviews: DHS is leading the interagency effort to develop and conduct comprehensive reviews of select potentially high-risk CI/KR. The Comprehensive Review Program spans multiple CI/KR sectors. Working collaboratively with the asset owner or operator, State and local law enforcement and first-responders, and other security partners, a DHS-led interagency team evaluates the potential consequences and vulnerabilities of a given asset or group of like assets from high-consequence and/or high-risk sectors within a specific geographical area, as well as the protective and response capabilities associated with the facility and the surrounding community.

Comprehensive Reviews will assist State and local jurisdictions in identifying vulnerabilities and capability gaps so they may be addressed in State and local homeland security strategies and CI/KR protection programs.

As the Comprehensive Review process matures, DHS expects to learn a great deal about the development and execution of joint programs, and to employ these lessons in building partnerships, thereby increasing the efficiency of Federal CI/KR protection activities, and reinforcing the value of a coordinated approach. Federal agencies with sector-based security responsibilities should plan and budget for participation in the Comprehensive Review Program.

Control Systems Security Initiative: DHS sponsors programs to increase the security of control systems, known as Supervisory Control and Data Acquisition (SCADA) systems. A control system is an interconnection of components (designed to maintain operation of a process or system) connected or related in such a manner as to command, monitor, direct, or regulate itself or another system. Control systems are embedded throughout the Nation’s CI/KR and may be vulnerable to increasing cyber threats that could have a devastating impact on national security, economic security, public health and safety, and the environment. The DHS Control Systems Security Initiative provides coordination efforts among Federal, State, Territorial, local, and tribal governments, as well as control system owners, operators, and vendors to improve control system security within and across all CI/KR sectors.

Federal Cyber System Security Programs: DHS established the Government Forum of Incident Response and Security Teams to facilitate interagency information sharing and cooperation across Federal agencies responsible for cyber system readiness and response. The members work together to understand

1 and manage computer security incidents and to encourage proactive and preventive security practices.
2 Other examples of Federal agency cybersecurity access control, certification, and policy enforcement tools
3 include:

- 4 ➤ The General Services Administration (GSA) is responsible for developing and implementing a
5 government-wide infrastructure for authentication services, an automated risk assessment tool for
6 government-wide use in certifying and accrediting its eAuthentication gateway. GSA is creating a
7 list of approved solution providers that supply smart cards based on Federal Public Key
8 Infrastructure standards and that include a new electronic authentication policy specification.
- 9 ➤ The National Oceanic and Atmospheric Agency (NOAA) has implemented enterprise-wide
10 vulnerability assessments and virus detection software, an intrusion detection system, anti-virus
11 scanning gateways, and a patch management policy.

12 **International Outreach Program:** DHS works with the Department of State to undertake international
13 outreach to foreign countries and international organizations to encourage the promotion and adoption of
14 best practices, training, and other programs as needed to improve the protection of overseas assets and
15 the reliability of the foreign infrastructures on which the United States depends.

16 **Internet Disruption Contingency Planning:** DHS formed a strategic partnership through the Internet
17 Disruption Working Group in January 2005 to coordinate cybersecurity contingency plans, including a plan
18 for recovering Internet functions. This working group collaborates with major security partners to identify
19 and prioritize the short-term protective measures necessary to prevent major disruptions of the Internet or
20 reduce their consequences, and to identify responsive/reconstitution measures for contingency plans in the
21 event of a major disruption.

22 **National Cyber Exercises:** DHS conducts exercises to identify, test, and improve coordination of the cyber
23 incident response community, including Federal, State, Territorial, local, tribal, and international
24 government elements, as well as private sector corporations and coordinating councils.

25 **National Cyber Response Coordination Group:** This entity facilitates coordination of the Federal
26 government's efforts to prepare for, respond to, and recover from cyber incidents of national significance
27 and other national cyber incidents and physical attacks that have significant cyber consequences
28 (collectively known as "cyber incidents"). The National Cyber Response Coordination Group serves as the
29 Federal government's principal interagency mechanism for operational information sharing and
30 coordination of the Federal government's response and recovery efforts during a cyber crisis. It uses
31 established relationships with the private sector and State and local governments to help manage a cyber
32 crisis, develop courses of action, and devise response and recovery strategies.

33 **Protective Community Support Program:** Specific advisory support is provided to the protective
34 community (e.g., law enforcement, first-responders), including training and exercise support.

35 **Protective Security Advisor (PSA) Program:** DHS protection specialists are assigned as liaisons
36 between DHS and the protective community at the state, local, and private sector levels representing major
37 concentrations of CI/KR across the United States. The PSAs are responsible for sharing risk information
38 and providing technical assistance to local law enforcement and the owners and operators of assets within
39 those areas.

1 **Site Assistance Visits (SAVs):** SAVs are facility security assessments designed to facilitate vulnerability
2 identification and mitigation discussions between the Federal government and individual owners and
3 operators of specific assets and resources. SAVs typically take one to three days to execute, and are
4 conducted jointly by a federally led team and facility owners and operators.

5 **Software Assurance:** DHS is developing best practices and new technologies to promote integrity,
6 security, and reliability in software development. DHS is leading the Software Assurance Program, a
7 comprehensive software assurance strategy that addresses processes, technology, and acquisition
8 throughout the software development life cycle to result in secure and reliable software that supports
9 mission requirements and enables more resilient organizations.

10 **3B.2 Guidelines, Reports, and Plans**

11 **Cybersecurity Plans:** Sector-specific cybersecurity plans are developed to assist SSAs in addressing
12 unique reliance on cyber systems and developing effective and appropriate cyber-protective actions.

13 **Educational Reports:** DHS provides several types of informational reports to support efforts to protect
14 CI/KR. They cover subjects such as the common vulnerabilities of CI/KR, potential indicators of terrorist
15 activity, and best practices for protective measures. As they are developed, these reports are distributed to
16 all State and Territorial Homeland Security Offices with the guidance that they should be shared with
17 owners and operators of CI/KR, the law enforcement community, and captains of the ports in their
18 respective jurisdictions.

19 **General Protection Plans:** Generally accepted standards of protection and protective measures for all
20 major classes of assets and special event venues are developed by all CI/KR security partners. They
21 include lessons learned and best practices from national-level vulnerability assessments that are shared
22 with law enforcement officials and industry to allow these parties to enhance the protection of assets that
23 are not nationally critical.

Appendix 3C: National Asset Database

3C.1 Why Do We Need a National CI/KR Inventory?

HSPD-7 directs the Secretary of Homeland Security to lead efforts to reduce the Nation's vulnerability to terrorism and deny the use of infrastructure as a weapon by developing, coordinating, integrating, and implementing plans and programs that identify, catalog, prioritize, and protect infrastructure in cooperation with all levels of government and private sector entities. A central Federal data repository for analysis and integration is required to provide DHS with the capability to identify, collect, catalog, and maintain a national inventory of information on assets, systems, and networks that may be critical to the Nation's well being, economy, and security.

To fulfill this need, DHS developed the National Asset Database (NADB), a continually evolving and comprehensive catalog of the assets, systems, and networks that comprise the Nation's infrastructure and other important resources. The NADB contains descriptive information regarding those assets and is the primary Federal repository for infrastructure information. Although the NADB is not a listing of prioritized assets, it has the capability to be queried in many ways that can help inform risk-reduction activities across the CI/KR sectors and government jurisdictions.

3C.2 How Does the Inventory Support the NIPP?

The NADB provides a coordinated and consistent framework to incorporate and display the CI/KR data submitted by Federal, State, and local agencies; the private sector; and integrated Federal or commercial databases. The framework and structure of the NADB have been constructed to readily integrate and provide the required data in a usable and effective manner. Two primary components of this framework are the categorization structure and the infrastructure type data fields:

- The **categorization structure** groups infrastructures by sector and identifies overlaps between and across sectors. It was developed in coordination with the SSAs to ensure that every infrastructure type is represented.
- The **infrastructure type data fields** outline the attributes of interest that are integral to assessment and analysis per a specific category of infrastructure. The information contained in these data fields feeds the strategic risk assessment process used to prioritize infrastructure.

The information in the NADB enables the analysis necessary to determine which assets, systems, and networks comprise the Nation's CI/KR, and to inform security planning and resource investments within and across sectors and governmental jurisdictions.

3C.3 What Is the Current Content of the Inventory?

DHS has gathered – and continues to gather – data related to the Nation's CI/KR from a variety of sources. The present inventory reflects a collection of information garnered from formal data calls and voluntary submissions from Federal agencies; State, Territorial, and local governments; and private sector entities, in addition to the inclusion of Federal and commercial databases as follows:

- **Liberty Shield List:** During the execution of Operation Iraqi Freedom, data were gathered for approximately 160 assets that formed the Department's Liberty Shield list and served as the foundation for the NADB. The Liberty Shield List was then supplemented by a set of data on more than 20,000 assets received from Federal agencies, voluntary State/Territory submissions, and commercial demographics products.
- **Protective Measures Target List (PMTL):** DHS utilized available data, external data sources, and subject matter experts to develop the PMTL of 1,700 assets as a focus for protective measures programs. In February 2004, the PMTL was sent to State and Local Homeland Security Advisors (SLHSA) for review to ensure relevancy and accuracy. After all additions and deletions were received in August 2004, DHS consolidated a new list of 1,849 assets defining the Buffer Zone Protection Program (BZPP).
- **Data Call:** DHS has worked directly with State and local governments to collect asset information to be included in the NADB. For instance, in July 2004, DHS conducted a data call of the 50 States and six Territories requesting that they provide a comprehensive listing of assets within their jurisdiction that they deem to be of national or local importance. In response, the States and Territories submitted information on more than 50,000 assets for possible inclusion in the NADB. DHS put out a similar data call to the SSAs in August 2005.

3C.4 How Will the Current Inventory Grow?

DHS continues to seek input from multiple sources, including existing databases managed by SSAs, commercial databases, State and local governments, and the private sector. Integrating existing databases will provide a dynamic common operating interface of infrastructure and vulnerability information through a cross flow of data between separate databases, or links to provide access to other databases. Existing databases being considered for integration are shown in Table 3C-1. Ownership and control of the data will be determined according to the circumstances of each database. Classification of the data will be based on the Original Classification Authority (OCA) guidance and will be protected as required by OCA guidance and direction.

Table 3C-1: Database Integration

Database	Use
Infrastructure and Critical Asset Viewer (iCAV)	DHS is leveraging existing geospatial capabilities and technology that is operating at the National Geospatial-Intelligence Agency (NGA) by implementing the iCAV as a DHS Geospatial Enterprise Solution for geospatial mapping, analysis, and sorting of the Nation's CI/KR. The iCAV system will use the geospatial component to spatially display and map information contained in the NADB.
iMapData	Web-based geospatial subscription service with access to more than 1,270 geo-referenced data sets covering physical infrastructure, emergency services, government facilities, political boundaries, military installations, media distribution areas, educational facilities, business locations, and demographic breakdowns.
National Threat Incident Database (NTIDB)	Source of consolidated information concerning credible threats and incidents presenting a danger to our Nation's critical infrastructure.
DHS LENS Vulnerability Databases	Unclassified Site Assistance Visit (SAV) reports, Common Vulnerability and Potential Indicator papers, and SAV and BZPP schedules. SAV and BZPP documents will be available through the classified and unclassified portals as applicable.
Commercial/Sector-Specific Databases	Existing Federal and commercial databases that contain the information sets pertinent to the NADB. Commercial databases will be purchased based on available funding and priorities for information requirements.

3C.5 How Will the Database Be Maintained?

The process of ensuring that the data collected is both current and accurate, and that user requirements are incorporated into the portal as necessary, is continual. Data updates and currency are largely dependent upon the sources of the data and the frequency of the updates that they provide.

Efficiency and reliability have been maintained through the implementation of unique numerical identifiers designed to facilitate the efficient integration of information from multiple databases. Verification and validation efforts by contracted companies or Federal employees will play a key role in ensuring information currency. Eventually, all approved users given access to the NADB will have the ability to provide updated information to the NADB Program Office for review prior to inclusion in the inventory.

Feedback forms are also incorporated to provide user recommendations, changes, requirements, and/or feedback to DHS. User requirements will help drive capabilities and functionalities of future evolutions and versions of the inventory.

3C.6 What Are Security Partner Roles and Responsibilities?

The development and population of the NADB is highly dependent on the participation and support of the SSAs, States, and private sector entities:

- SSAs have primary responsibility for providing sector information to DHS for inclusion in the NADB using the format, data schema, and categorization system employed by the NADB.¹³ Their processes for sector infrastructure and database identification in coordination with security partners will be described in the SSPs.
- Some State governments have either already developed infrastructure databases or begun the process to identify and assess infrastructure within their jurisdictions. State governments should work closely with DHS and SSAs to ensure that data collection efforts are streamlined and coordinated.
- The most current and accurate data are best known by the owners and operators themselves. Thus, as the owners and operators of the majority of the Nation's infrastructure, private sector entities are encouraged to be actively involved in the development and population of the NADB. Primarily through the provision of asset information and industry-specific subject matter expertise, the private sector is playing an integral role in the development of the NADB.

3C.7 What Are the Future Plans for NADB Expansion?

The current NADB incorporates a flexible design to facilitate evolution, growth, and continued interconnectivity with additional databases and tools. Advancements will include integration with multiple commercial and Federal infrastructure databases, vulnerability assessment tools and libraries, intelligence and threat reporting databases, and geospatial tools into a single, integrated, Web-based portal.

¹³ The DHS/IP taxonomy is the foundation for multiple DHS programs that focus on critical infrastructure, such as the NADB and the National Threat Incident Database, and should be the foundation outlined within the SSPs. This common framework will allow more efficient integration and transfer of information, as well as a more effective analytical tool for making comparisons.

1 DHS is developing the next-generation NADB with a more versatile platform to even better support
2 integration of DHS and SSA mission-specific applications and mission-specific databases. The goal of this
3 effort is to create an asset database that more efficiently and effectively supports the implementation of
4 NIPP risk management framework activities, including:

- 5 • Integration of vulnerability, consequence, and asset attribute data into a single portal interface to be
6 used as the foundation for the NIPP risk assessment process;
- 7 • Access to threat data to support the development of asset and system risk scores;
- 8 • Assessment and, if appropriate, prioritization of assets and systems across sectors and jurisdictions
9 based on risk to promote the more effective allocation and use of available resources and to inform
10 planning and threat response actions at all levels of government and the private sector;
- 11 • Sharing of consistent information so that all partners involved in homeland security operate from a
12 common frame of reference with consistent information;
- 13 • Acting as a primary information and integration hub for protective security needs throughout the country
14 in support of DHS- and SSA-led activities;
- 15 • Supporting the efforts of law enforcement agencies during National Security Special Events and other
16 high-priority security events; and
- 17 • Supporting the efforts of primary Federal agencies to respond to and recover from major natural or
18 terrorist-caused disasters.

- 1 Appendix 4: Organizing and Partnering for CI/KR Protection
- 2 Appendix 4A: Existing Coordination Mechanisms
- 3 Appendix 4B: Protected Critical Infrastructure Information (PCII) Program

1 Appendix 4A: Existing Coordination Mechanisms

2 The coordination mechanisms established under the NIPP serve as the primary means for coordinating
3 CI/KR protection activities nationally. However, many other avenues exist for security partners to engage
4 with each other and government at all levels to ensure that their efforts are fully coordinated. The following
5 table summarizes many of these available mechanisms.

Coordination	Mechanism	Description
Local to Local	Inter-Local Agreements	Cities and towns can exchange information and cooperate on any number of projects. Inter-local agreements are a mechanism to do cooperatively anything that can be done as an individual municipality.
	Mutual-Aid Agreements	Established means through which one local government can offer assistance and another receive assistance in a time of disaster. These agreements cover logistics, deployment, liability, reimbursement, and many other issues. The intent is to provide assistance in the most efficient manner possible by having the terms and conditions worked out in advance.
	County Commissioner Interaction	Because counties are the level of government closest to the people and they serve all the people of the State, county commissioners provide leadership, services, and programs to meet the health, safety, and welfare needs of their citizens.
Local to State	Committees, Commissions, and Boards	Local to State legislative- and regulatory-level interactions occur through State committees, commissions, and boards dealing with environmental, transportation, community development, retirement, insurance, and many other issues. This also includes working with the office of the Governor, Homeland Security Advisor, or Emergency Management Agency.
Local to Federal	Associations	National associations of local governments serve as a bridge between local elected officials and the Federal government to ensure that the public safety and homeland security needs of localities are met. These organizations, such as the National League of Cities, the National Association of Counties, and the U.S. Conference of Mayors, work to ensure that Federal resources are provided for disaster planning, mitigation, and recovery.
State to State	Intrastate Councils of Government	Councils of State Governments are regional councils that, by law, are political subdivisions of the State with the authority to plan and initiate needed cooperative projects; however, they do not have the power to regulate or tax because these authorities are exclusively assigned to cities and counties. A council's duties may include comprehensive planning for regional employment and training needs, criminal justice, economic development, homeland security, emergency preparedness, bioterrorism, 911 service, solid waste, aging, transportation, and rural development.
	Interstate Compacts	States face issues that are not confined to geographical boundaries or jurisdictional lines. Interstate compacts are a mechanism that can be used to address sector interdependencies and coordinate protection of CI/KR. Compacts are organized in a number of ways: <ul style="list-style-type: none"> ▪ Sector-based compacts focus on specific CI/KR resources that are shared or are interdependent across State boundaries (e.g., the Western Interstate Energy Compact); ▪ Preparedness-focused compacts, such as the Interstate Mutual-Aid Compact, establish a means for participating jurisdictions to provide voluntary assistance to other States in response to an event that overwhelms the resources of State and local governments; and ▪ Regional compacts provide a means for participating jurisdictions to coordinate activities within a specific geographical area that spans multiple

Coordination	Mechanism	Description
		<p>States. These agreements, such as the Canadian River Compact, define the specific equities of each State within the particular region.</p> <p>For more information on interstate compacts, contact the National Center for Interstate Compacts (NCIC): http://www.csg.org/CSG/Programs/National+Center+for+Interstate+Compacts/default.htm.</p>
State to Federal	Associations	Organizations such as the National Governors Association, the National Conference of State Legislatures, and the Council of State Governments represent the interests of States during the Federal policymaking process. Additionally, these groups support State leaders by keeping their members informed of key Federal decisions that impact State government.
	State Liaison Offices	Some States have formed specific liaison offices in Washington, D.C., to maintain awareness of Federal developments and ensure that their individual State perspective is represented in the Federal policymaking process. These offices report back regularly to their State's leadership and legislature regarding Federal issues of interest.
Federal to Federal	Memoranda of Understanding or Agreement	Agreements between two or more Federal departments and agencies to cooperate on a specific topic or initiative.
Private Sector to Government (all levels)	Public-Private Partnerships	Contractual agreement between a public agency (i.e., Federal, State, or local) and a private sector entity. Through this agreement, the skills and assets of each sector (public and private) are shared in delivering a service or facility for the use of the general public.
	Advisory Councils, Boards, and Commissions	In addition to the SCCs and ISACs, a variety of private sector organizations exist that focus on homeland security and infrastructure protection activities on a sector and geographical basis. These groups are made up of members of the public and subject matter experts, and provide advice and recommendations to governments at all levels.
	Associations	Myriad private sector associations exist that advocate on behalf of their members in the policymaking process at the Federal, State, and local levels. These groups are comprised of individuals or companies with common interests. Because of their ability to communicate with their members, private associations provide an effective means for government to provide information to the public and also to learn the concerns of specific groups of security partners.

Appendix 4B: Protected Critical Infrastructure Information (PCII) Program

Implementation of the NIPP will rely greatly on critical infrastructure information provided by the private sector. Much of this information is business or security sensitive and could cause serious economic or public safety damage if improperly disclosed to the public. The Protected Critical Infrastructure Information (PCII) Program provides a means for sharing private sector information with the government while providing the assurances that the information will be exempt from public disclosure and properly safeguarded.

The PCII Program operates under the authority of the Critical Infrastructure Information Act of 2002 (hereafter, "the Act"). The existing interim rule, 6 CFR Part 29, defines the requirements for submitting critical infrastructure information. The rule also defines the requirements that government entities must meet for accessing and safeguarding PCII. The PCII Program enables the sharing of private sector information with government entities by offering protection from disclosure under the Freedom of Information Act, State and local disclosure laws, and use in civil litigation or regulatory action. For more information or to arrange a meeting to further discuss PCII, please contact the PCII Program Office at pcii-info@dhs.gov. Additional PCII Program information may also be found at www.dhs.gov/pcii.

DHS established the PCII Program Office to manage information, develop protocols for how to care for "voluntarily submitted critical infrastructure information," and raise awareness regarding the removal of impediments to information sharing regarding cyber and infrastructure vulnerabilities between the public and private sectors.

The PCII Program Office is responsible for receiving, validating, and safeguarding critical infrastructure information submitted to DHS. The Program Office establishes partnerships with government users of critical infrastructure information private sector and entities willing to share their information on a voluntary basis. Government entities seeking to access PCII must meet safeguarding requirements as defined by the Program Office.

4B.1 Critical Infrastructure Information (CII) Protection

The following general process applies for CII submissions:

- The PCII Program Office will first validate that the information qualifies for protection under the Act;
- All validated PCII will be stored in a secure data management system. All original PCII remains in the data management system, and only copies are shared with authorized users. Secure methods will be used for disseminating PCII;
- Authorized users must comply with safeguarding requirements defined by the PCII Program Office; and
- Any suspected disclosure of PCII will be promptly investigated. Federal employees may face significant fines or penalties for improper disclosure.

4B.2 Potential Uses of PCII

PCII may be shared with authorized government entities for the purposes of securing critical infrastructure and protected systems. PCII will be used for analysis, prevention, response, recovery, or reconstitution of CI/KR threatened by terrorism or other hazards:

- Authorized government entities may generate advisories, alerts, and warnings relevant to the private sector based on the information provided. Any communications made available to the public must not contain any sensitive information provided by the submitter; and
- PCII can be combined with other information, including classified information, to construct actionable knowledge. All PCII used in such products must be marked accordingly.

4B.3 Validation of PCII

Individuals or collaborative groups may submit Critical Infrastructure Information (CII) for protection purposes. Representatives of corporations, privately held companies, non-government organizations, and private citizens, as well as representatives of State and local governments, may also submit information for protection purposes. The Act also allows collaborative groups, whether they are formal or informal, to come together to collaborate and submit CII for protection purposes.

In support of the NIPP, the PCII Program Office will work with other DHS offices to determine how to efficiently process specific types of CII submissions for PCII protection.

In order to be validated as PCII, the information:

- Must be submitted voluntarily to the PCII Program Office or the PCII Program Office's delegates;
- Cannot be submitted in lieu of independent compliance with a Federal legal requirement;
- Must not be customarily in the public domain;
- Must be related to known or perceived threat, or ability to resist, recover, repair, or respond to the vulnerabilities of critical infrastructures; and
- Must be accompanied by an Express Statement and Certification statement as required by law, attesting to the above.

The submitted information enjoys the presumption of protection and is safeguarded as PCII unless the PCII Program Office or other designated validating authority determines otherwise. If it is determined that a submission may not qualify for protection under the Act, the submitter is given an opportunity to provide additional information explaining why the submission qualifies for protection under the Act. If the submission is ultimately rejected and is not validated as PCII, it will be destroyed in accordance with the submitter's instructions.

4B.4 PCII Program Protections

The PCII Program has established procedures to ensure that PCII is properly accessed, used, and safeguarded. PCII Program safeguards ensure that all information submitted for protection is properly protected throughout its life cycle. These safeguards ensure that submitted information is:

- Used appropriately for homeland security purposes;
- Accessed only by authorized and properly trained staff of Federal, State, or local government agencies with a lawful and authorized need to know, as stated in the Act;
- Protected from disclosure under the Freedom of Information Act and similar State and local disclosure laws, and use in civil litigation and regulatory actions; and
- Safeguarded and handled in a secure manner that protects PCII from unauthorized access.

4B.5 Authorized Users

Only authorized users can access PCII. Authorized users consist of Federal, State, or local government employees or contractors supporting Federal agencies. All users must:

- Be engaged in activities specified in the Act;
- Have a need to know;
- Be trained in PCII handling and safeguarding requirements; and
- In the case of any non-Federal government employee, sign a Non-Disclosure Agreement acknowledging his or her obligation to properly handle and safeguard PCII.

In addition, non-DHS Federal agencies and State or local government entities must sign a Memorandum of Agreement acknowledging their responsibility to properly handle and safeguard PCII.

4B.6 Accreditation of Entities That Will Receive PCII

To support proper safeguarding and protection of PCII, all Federal, State, and local government entities must be accredited before accessing PCII. The accreditation process ensures consistent application of uniform PCII Program standards and minimum requirements by all participating entities. In addition, the accreditation process ensures that users understand the handling, use, dissemination, and safeguarding of PCII, and have the necessary resources for operating a PCII Program. These standards, which include requirements for receiving, securing, disseminating, and destroying PCII, are detailed in the *PCII Program Procedures Manual*.

Each entity must have a PCII Officer and Deputy PCII Officer who oversee the PCII Program within the entity. They must attend a three-day training course and pass a written exam. In addition, entities can designate Assistant PCII Officers to assist in overseeing multiple sites or a large program within one site. Organizations receiving PCII must be engaged in authorized activities as specified in the Act and the Regulation.

1 The PCII Program Office oversees the accreditation process, including visiting entities' sites to ensure that
2 they are meeting the requirements for being accredited. The Program Office ensures that PCII is
3 disseminated only to those entities that have satisfied the accreditation requirements or that are specifically
4 authorized by submitters to access their PCII.

5 **4B.7 Penalties for Intentionally Mishandling PCII**

6 The law and rule prescribe criminal penalties for intentional unauthorized access, distribution, and misuse
7 of PCII:

- 8 • Federal employees may be subject to disciplinary action, including criminal and civil penalties and loss
9 of employment; and
- 10 • Contract employees may face termination and the contractor may have its contract terminated.
- 11 • Sanctions do not apply directly to State and local officials or employees; however, State and local
12 participating entities may have their own penalties for improperly handling of sensitive information that
13 they may apply to these actions. The State will face losing future access to PCII.

14 **4B.8 Status of the PCII Program**

- 15 • The PCII Program is currently operating under an interim rule. A final rule is expected in 2006.
- 16 • The PCII Program Office is working to seamlessly integrate PCII protections into information-sharing
17 programs within DHS/OIP. Ongoing projects include:
 - 18 ➤ Risk Assessment Methodology for Critical Asset Protection (RAMCAP);
 - 19 ➤ Homeland Security Information Network – Critical Sectors (HSIN-CS);
 - 20 ➤ Constellation; and
 - 21 ➤ Chemical Sector Comprehensive Reviews.
- 22 • One option the private sector has for submitting CII is through a secure Web portal accessed from the
23 PCII Program Web site (<https://submitcii.dhs.gov/pcii>).
- 24 • The PCII Program is conducting a stakeholder analysis of users and submitters to adjust and improve
25 program processes and procedures.
- 26 • On-line training provides individuals seeking access to PCII with an easy-to-use, self-paced course.
27 The PCII Program Office provides PCII Officers, Deputies, and Assistants with instructor-led training to
28 help entities achieve accreditation.

- 1 Appendix 5: Integrating CI/KR Protection as Part of the Homeland Security Mission
- 2 Appendix 5A: Sector Overview
- 3 Appendix 5B: Sector-Specific Plan Content Summary
- 4 Appendix 5C: State, Territorial, Tribal and Local Government Considerations
- 5 Appendix 5D: Recommended Homeland Security Practices for Use by the Private Sector

Appendix 5A: Sector Overview

The sections that follow present a short overview of each of the 17 CI/KR sectors. Additional information can be found in each of the SSPs.

5A.1 Agriculture and Food Sector

The Agriculture and Food Sector accounts for roughly one-fifth of the Nation's economic activity and has the capacity to provide food and clothing to people beyond the U.S. borders. The Sector is overseen at the Federal level by the U.S. Department of Agriculture (USDA) and the U.S. Department of Health and Human Services' Food and Drug Administration (FDA). The Sector is almost entirely privately owned and covers agricultural production from pre-harvest through post-production and national forest lands, the animal feed industry, and food facilities. The Sector includes an estimated 2.1 million farms, an estimated 880,587 firms, and 1,086,793 facilities. The Sector also covers food aid that the U.S. government gives for humanitarian purposes.

5A.2 Banking and Finance Sector

The Banking and Finance Sector, the backbone of the world economy, is a large and diverse sector primarily owned and operated by private entities. The banking system consists primarily of Federal and State-chartered depository institutions. In most cases, Federal regulators have at least some authority over these institutions. Financial services firms provide a broad array of financial products that: (1) allow customers to deposit funds and make payments, (2) provide credit and liquidity, (3) allow customers to invest funds for both long and short periods, and (4) transfer financial risks between customers. Key banking system assets include retail facilities, ATM networks, Automated Clearing House operators, Federal Reserve Banks, and electronic payment networks. Credit and liquidity markets are not formal markets with either a physical location or one narrow set of methods that define them, yet they are fundamental to the operation of the U.S. economy and Federal and State governments. Investment products are offered by a wide variety of financial institutions, such as securities firms, depository institutions, pension funds, and government-sponsored enterprises. Risk-transfer products are offered by insurance companies, futures firms, and forwards participants. The Sector is overseen at the Federal level by the U.S. Department of the Treasury.

5A.3 Chemical Sector

The Chemical Sector consists of four main segments, based on the end product produced: (1) basic chemicals, (2) specialty chemicals, (3) life sciences, and (4) consumer products. There are several hundred thousand chemical facilities in the United States, encompassing everything from production facilities to hardware stores. The great majority of these facilities are privately owned, requiring DHS, as the SSA, to work closely with the private chemical industry and its industry associations in order to identify assets, assess risks, prioritize assets, develop protective programs, and measure program effectiveness.

More than 15,000 U.S. facilities produce, use, or store more than 140 chemicals that, when present above certain threshold amounts, have the potential to pose great risk to human health and the environment if released. Only one Federal law, the Maritime Transportation Security Act of 2002 (46 USC § 70101, et

seq.), establishes direct authority concerning terrorism-related security at chemical facilities in the maritime domain. Consequently, the decision to secure chemical facilities overwhelmingly lies with the individual asset owners and operators, although a few States and localities have begun enacting regulations addressing chemical facility security. In addition, a considerable number of Federal laws impose safety or other requirements on the production, storage, use, and transportation of chemicals – indirectly helping to secure chemical facilities.

5A.4 Commercial Facilities Sector

The Commercial Facilities Sector comprises a number of asset categories, including hotels, commercial office buildings, public institutions (e.g., museums, libraries, zoos), convention centers/stadiums, theme parks, schools, colleges, apartment buildings, restaurants, and shopping centers. With more than 53,000 hotels, 46,000 shopping centers, and 1,300 stadiums, commercial facilities, sometimes known as “soft targets,” are potential targets for terrorist attacks because they are especially vulnerable and may be subject to a large number of casualties and economic damage. Due, in part, to accessibility, commercial facilities are very difficult to defend against terrorist attacks. DHS is the SSA for the Commercial Facilities Sector, in coordination with industry associations and other sector security partners.

5A.5 Dams Sector

The Dams Sector includes levees, more than 77,000 conventional dams, navigation locks, canals (excluding channels), or other similar types of water retention structures. Although many infrastructures (e.g., roads, bridges, sewer systems) are owned by public entities, approximately 66 percent of the dams in the United States are owned by private entities. Very large dams (i.e., over one million acre-feet) are mostly owned by the Federal government. Private companies or cooperatives own most medium-sized (i.e., 100 to 10,000 acre-feet) dams that are used for irrigation, water supply, hydroelectric power, and direct hydropower. Most small dams (i.e., less than 100 acre-feet) are owned by the private sector. State dam safety agencies have jurisdiction over approximately 95 percent of the dams in the United States, while Federal agencies regulate approximately five percent of U.S. dams. DHS is the SSA for the Dams Sector.

5A.6 Defense Industrial Base Sector

The Defense Industrial Base (DIB) Sector provides defense-related products and services that are essential to mobilize, deploy, and sustain military operations. The DIB includes more than 100,000 companies (both domestic and foreign entities, some with operations located in many countries) and their subcontractors to provide incidental materials and services under contract to the Department of Defense (DOD), as well as facilities (government-owned, contractor-operated/government-owned, and government-operated). SSA responsibility for the DIB sector is assigned to the DOD. Sector security partners include the other government entities and the worldwide industrial complex with the capabilities of performing research and development, design, production, and maintenance of military weapons systems, subsystems, components, or parts to meet military requirements. Responsibility for the DIB sector is assigned to the DOD. Note that the DIB does not include commercial infrastructure that provides, for example, power, communications, transportation, and other utilities that DOD war fighters and support organizations use to meet their respective operational needs. These activities, including cyber, are

addressed in DOD's broader Defense Critical Infrastructure Program (DCIP) and are integrated into all DIB Sector activities.

5A.7 Emergency Services Sector

The Emergency Services Sector consists of five disciplines: (1) emergency management, (2) emergency medical services, (3) fire and hazardous materials, (4) law enforcement, and (5) search and rescue. The Emergency Services Sector is a system of response elements that forms America's first line of defense and prevention in any terrorist attack or other disaster. The core elements of the Sector are not found in large, complex structures or facilities, but in the highly trained forces of professionals organized and equipped to conduct high-risk operations in times of emergency. In addition, emergency services include key facilities such as 911 centers, Emergency Medical Services (EMS)/fire stations, transport vehicles, and data systems. The ability of the Nation to protect all CI/KR is heavily dependent on these men and women who serve in the Nation's emergency services. DHS is the SSA for the Emergency Services Sector.

5A.8 Energy Sector

The Energy Sector is divided into three key segments--electricity, petroleum, and natural gas--that are closely interrelated (for example, natural gas is a key fuel for electricity production). The Department of Energy is the SSA for the Energy Sector. More than 80 percent of the country's energy infrastructure is owned by the private sector.

The U.S. electricity segment contains 5,000 power plants with approximately 905 gigawatts of generating capacity. Approximately 50 percent of electricity is produced by combusting coal (primarily transported by rail), 20 percent is generated in nuclear power plants, and 18 percent is produced by combusting natural gas. The remaining generation is provided by hydroelectric plants (seven percent), oil (two percent), and by renewable (solar, wind, geothermal) and other sources (three percent). Electricity generated at power plants is transmitted over 158,000 miles of high-voltage transmission lines and distributed to 131 million customers over millions of miles of lower voltage distribution lines.

The petroleum segment entails the exploration, production, storage, transport, and refinement of crude oil. The crude oil is refined into petroleum products that are then stored and distributed to key economic sectors throughout the United States. Key petroleum products include motor gasoline, jet fuel, distillate fuel oil, residual fuel oil, and liquefied petroleum gases. Both crude oil and petroleum products are imported, primarily by ship, as well as produced domestically. Currently, 63 percent of the crude oil required to fuel the U.S. economy is imported. In the United States, there are more than 500,000 crude oil producing wells, 30,000 miles of gathering pipeline, and 74,000 miles of crude oil pipeline. There are 152 petroleum refineries, 95,000 miles of product pipeline, and 2,000 petroleum terminals.

Natural gas is also produced, piped, stored, and distributed in the United States. Increasingly, natural gas is imported as liquefied natural gas (LNG). There are more than 383,000 gas production and condensate wells and 45,000 miles of gathering pipeline in the United States. Gas is processed at 726 gas processing plants, and there are more than 254,000 miles of interstate pipeline for the transmission of natural gas. Gas is stored at 410 underground storage fields and 96 LNG storage facilities. Finally, natural gas is distributed to homes and businesses over 981,000 miles of distribution pipelines.

5A.9 Government Facilities Sector

The Government Facilities Sector includes facilities that are typically built, leased, or otherwise acquired to perform a specific departmental or agency mission at the Federal, State, and local levels. A facility can consist of one building or multiple buildings on the same site. In many cases, it is important to note that such facilities serve as shells protecting mission-critical assets within. All facilities fall into three basic categories: (1) domestic (non-defense) facilities, which are owned and managed by a Federal department or agency or by State, Territorial, or local government; (2) defense facilities, which are owned and managed by the DOD that do not fall under the General Services Administration (GSA) or other specific department or agency management; and (3) overseas facilities, which are located outside U.S. national borders. DHS is the SSA for the Government Facilities Sector.

5A.10 Information Technology Sector

The Information Technology (IT) Sector produces hardware, software, and services that enable other sectors to function. For example, the IT Sector produces laptops, operating systems, and Internet search engines. These IT Sector products are consumed across other critical infrastructure sectors and the government. The production of hardware, software, and services therefore defines the IT Sector; the IT Sector may be considered as the "IT Industrial Base." The Internet is a key resource composed of assets within both the IT and Telecommunications sectors and is used by all sectors in varying degrees of business and operational dependence. DHS is the SSA for the IT Sector.

5A.11 National Monuments and Icons Sector

The National Monuments and Icons (NM&I) Sector encompasses a diverse array of assets located throughout the United States and its Territories. While many of these assets are listed in either the National Register of Historic Places or the List of National Historic Landmarks, all share three common characteristics: (1) they are a monument, physical structure, object, or geographical site; (2) they are widely recognized to represent the Nation's heritage, traditions, or values, or widely recognized to represent important national cultural, religious, historical, or political significance; and (3) their primary purpose is to memorialize or represent some significant aspect of the Nation's heritage, tradition, or values, and to serve as points of interest for visitors and educational activities. Some physical structures that could be considered as monuments or icons (e.g., Golden Gate Bridge, Sears Tower, Hoover Dam, and the U.S. Capitol) have been determined to be more appropriately assigned to other sectors, such as Transportation, Commercial Facilities, Dams, and Government Facilities, because of their primary purpose. The Department of the Interior is the SSA for the NM&I Sector.

5A.12 Nuclear Reactors, Materials, and Waste Sector

Responsibility for the coordination of the Nuclear Reactors, Materials, and Waste Sector was designated in HSPD-7 to DHS in close cooperation with the Nuclear Regulatory Commission. This Sector includes the Nation's 104 commercial nuclear reactors licensed to operate in 31 States. Nuclear power accounts for approximately 20 percent of the Nation's electrical generating capacity. As noted in HSPD-7, this Sector also includes non-power nuclear reactors used for research, testing, and training; nuclear materials (source, byproduct, and special nuclear materials) used in medical, industrial, and academic settings;

nuclear fuel fabrication facilities; the decommissioning of reactors; and the transportation, storage, and disposal of nuclear materials and waste. Although some of these activities are not considered CI/KR by themselves, radioactive materials stolen from them could be used against other CI/KR.

5A.13 Postal and Shipping Sector

The Postal and Shipping Sector moves hundreds of millions of messages, products, and financial transactions each day. Postal and shipping activity is differentiated from general cargo operations, which is part of the Transportation Sector, by its focus on small and medium-sized packages and by service from millions of senders to millions of destinations. The Sector is highly concentrated, with a handful of providers holding a market share of more than 95 percent. However, Sector protection requires the involvement of more than just the delivery firms. Customers and other service firms are integrally involved in the value chain through the creation of sent items, work sharing such as pre-sort and drop-shipment, and mailroom operations. The web of Sector providers, customers, and service firms extends internationally, posing important security challenges, including customs inspections. The DHS Transportation Security Administration (TSA) is the SSA for the Postal and Shipping Sector.

5A.14 Public Health and Healthcare Sector

The Public Health and Healthcare Sector is highly decentralized and loosely coupled. It consists of State and local health departments, hospitals, health clinics, mental health facilities, nursing homes, blood-supply facilities, laboratories, mortuaries, medical and pharmaceutical stockpiles, and supporting personnel. The United States 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 Strategic National Stockpile. These elements of the Sector are present in virtually all U.S. communities and respond to nearly all conceivable attacks or related disasters. The Department of Health and Human Services, as the designated Federal agency responsible for coordinating the efforts of the Sector, will work with sector security partners to minimize vulnerabilities to security threats.

5A.15 Telecommunications Sector

Over the past 20 years, the Telecommunications Sector has evolved from being predominantly a provider of equipment and voice services into a diverse, competitive, and interconnected industry. DHS is the SSA for this sector. The Telecommunications Sector has four broad components:

- **Wireline Communications:** Primarily consists of the public switched telephone network (PSTN), but also includes cable networks and enterprise networks. The PSTN is a domestic telecommunications network accessed by telephones, key telephone systems, private branch exchange trunks, and data arrangements. These components are connected by nearly two billion miles of fiber and copper cable (physical), information technology systems that monitor and move the data (cyber), and dedicated staff to ensure service (people).
- **Wireless Communications:** Includes cellular telephone, paging, personal communications services, high-frequency radio, and other commercial and private radio services.

- **Satellite Communications:** Uses a combination of terrestrial and space components to deliver various telecommunications, Internet data, and video services.
- **Public Safety Answering Points and 911:** Require both wireline and wireless for access to the emergency services system.

5A.16 Transportation Sector

The Nation's transportation system quickly, safely, and securely moves people and goods through the country and overseas. DHS/TSA is the SSA for the Transportation Sector, which consists of six key sub-sectors or modes:

- **Aviation:** Includes aircraft, air traffic control systems, and approximately 450 commercial airports and 19,000 additional airfields. Additionally, this mode includes civil and joint-use military airports, heliports, short takeoff and landing ports, and seaplane bases.
- **Highway:** Encompasses more than four million miles of roadways and supporting infrastructure (bridges, tunnels, interchanges, traffic management centers, terminals, transfer points, and facilities). Vehicles include cars, buses, motorcycles, and all types of trucks.
- **Maritime:** Includes vessels, ports, inland waterways, harbors, navigable waters, the Great Lakes, Territorial seas, contiguous waters, customs waters, coastal seas, littoral areas, piers, wharves, aids to navigation, critical maritime infrastructure, and sea lanes and maritime approaches to the United States.
- **Mass Transit:** Includes multiple-occupancy vehicles designed to transport customers on local and regional routes (e.g., transit buses, trolleybuses, vanpools, ferryboats, monorails, heavy (subway) and light rail, automated guideway transit, inclined planes, and cable cars).
- **Pipeline Systems:** Includes vast networks of pipeline that traverse hundreds of thousands of miles throughout the country, carrying nearly all of the Nation's natural gas and about 65 percent of the hazardous liquids (crude and refined oil products), as well as various chemicals.
- **Rail:** Consists of hundreds of railroads, more than 143,000 route miles of track, more than 1.3 million freight cars, and roughly 20,000 locomotives. Amtrak operates more than 22,000 route miles in 46 States and Washington, D.C., and has some 500 station stops.

5A.17 Water Sector

The Water Sector includes both drinking water and wastewater utilities. There are approximately 160,000 public water systems in the United States. These systems serve 84 percent of the U.S. population. Wastewater is treated by publicly owned treatment works and by private facilities. There are more than 16,000 publicly owned treatment works that serve 75 percent of the U.S. population. The EPA was designated in HSPD-7 as the SSA for the Water Sector. Many of EPA's ongoing programs also support security-related activities. This Sector is vulnerable to a variety of attacks through contamination with deadly agents, the release of toxic gaseous chemicals, and other means that could result in thousands of casualties, and/or the loss of water to support economic activity, fire fighting, and other critical services. The broad-based strategy to address the security needs of the entire Water Sector is comprised of four key initiatives: (1) risk identification; (2) protection and preparedness; (3) response, recovery, and

- 1 decontamination; and (4) research. The work includes providing support to utilities by preparing
- 2 vulnerability assessment and emergency response tools, providing technical and financial assistance, and
- 3 information exchange.

Appendix 5B: Sector-Specific Plan Content Summary

The SSPs follow a consistent structure to facilitate cross-sector comparisons and enable coordination among security partners. More detailed directions are provided to the SSAs on the development and implementation of SSPs through technical assistance sessions and guidance documents. If an SSA determines that the information needed to adequately describe sector processes is too sensitive to be made public, they may elect to generate a classified annex to the SSP. Each Plan includes the following content:

Letters of Agreement and Support

Letter of Instruction

Executive Summary

Table of Contents

Introduction:

- Purpose of the SSP;
- Scope and applicability;
- Goal and objectives (support of the NIPP Goal and Objectives and sector security goals and cross-sector priorities);
- Planning assumptions; and
- Review of authorities: Information on governing authorities (e.g., laws, rules, regulations, directives, executive orders, etc.) applicable to the protection of infrastructure within the sector, and any gaps in authorities that could hinder the CI/KR protection process related to information collection, sharing and protection, vulnerability assessment, and protective strategies.

Chapter 1: Sector Characteristics and Relationships

- Definition of sector infrastructure boundaries, including the categorization that was prepared in coordination with DHS. Recognition of the complexity and diversity of the sector by including subcategories or classes of infrastructure, particularly if the sector includes obviously distinct types of operations, businesses, facilities, etc.
- Characteristics of the infrastructure, including special considerations that may be associated with physical, cyber, or human elements and international linkages.
- Sector “snapshot” that highlights sector-specific threats.¹⁴
- Relationships with other sectors (caused by overlap or interdependency) and how this is addressed.

¹⁴ Sector threat information will be provided by DHS as discussed in Chapter 3.

- Status of current security partner relationships (identify successful efforts and target areas where further outreach is desired).
- Definition of sector security partners and their roles and responsibilities.
- Sector leadership and coordination, including structures, mechanisms, and status.
- Information-sharing and protection structures and mechanisms through which information will be shared and protected within the sector, with other sectors, and with DHS, establishing the case for the private sector to share the information with the SSA and DHS.

Chapter 2: Set Security Goals

- Summary of the process used to develop the vision and goals in the SSP and how they will be re-evaluated as the sector changes.
- Outcome of the process in terms of the agreed-upon sector security vision, goals, and any associated objectives.
- Summary of initiatives that are cross sector in nature, essential to achieving sector security goals, and require coordination with other SSAs.

Chapter 3: Identify Infrastructure

Current or proposed approaches for:

- Defining the sector-specific information that will be collected (e.g., characteristics, dependencies and interdependencies, international links, and cyber systems needed for it to function) and the criteria for identifying infrastructure requiring further analysis;
- Identifying currently available information on sector and cross-sector infrastructure; formatting, linking, and delivery of data to DHS; and location, protection, and updating of information; and
- Ensuring that the information collected is reliable through verification, review, and correction of information, and follow-up activities required based on the infrastructure's significance (e.g., onsite meetings, validation of owner/operator procedures, etc.).

Chapter 4: Assess Risks

Current or proposed approaches for implementing a common risk management vocabulary, threat scenarios, scales, and generally accepted risk assessment practices; and the process for:

- Identifying, collecting, and protecting current consequence, vulnerability, threat, and risk assessment data;
- Identifying and assessing sector-specific tools;
- Building a risk analysis capability;
- Encouraging security partner implementation; and
- Assisting in dependency and interdependency analysis.

Chapter 5: Prioritize

Discussion of the process, resulting in a validated assessment of component risk factors (threat, vulnerabilities, and consequences) with known inter- and intra-sector dependencies and interdependencies to produce an assessment of those assets representing national risk. Include any uncertainties that may lead to difficulties in producing the assessment.

Chapter 6: Implement Protective Programs

Discussion of current or proposed processes for developing protective programs to implement selected strategies. Describe:

- Sector security strategies that balance prevention, protection, response, and recovery by sector, subsector, or infrastructure class and how they influence guidelines or best practices for protective actions;
- Decision-making processes for assessing the anticipated costs of protective actions, including purchasing data sources, balancing costs against the risks to particular assets, and the role of security partners in carrying out these analyses;
- Description of best practices that may be appropriate for sector infrastructure and how they are shared and used to encourage security partner implementation;
- Coordination of sector-specific protective actions with actions implemented by DHS;
- Roles and responsibilities of sector security partners; and
- Protection of information on risk to infrastructure.

Chapter 7: Measure Progress

- Process for developing sector-specific metrics based on its CI/KR protection goals to result in a short, focused, and manageable list of process and outcome metrics.
- Responsibilities and timeframes for meeting reporting requirements.
- Description of processes to continuously refine CI/KR protection efforts, including:
 - Comparing performance to goals;
 - Revising approaches in the SSP to reflect activities and progress;
 - Identifying and improving upon protection of assets that warrant additional resources or other changes;
 - Focusing CI/KR protection efforts on addressing areas of concern; and
 - Collecting and sharing how lessons learned and best practices are shared with security partners and DHS.

Chapter 8: Long-Term Sector CI/KR Protection Elements

- Awareness, training, and education.

- Research and development – How the sector will:
 - Identify sector technology requirements and communicate them to the DHS Science and Technology (S&T) Directorate/Office of Science and Technology Policy (OSTP) for inclusion in the Federal CI/KR R&D Plan on an annual basis, and provide a summary of technology requirements;
 - Annually solicit a listing of current Federal R&D initiatives from the DHS S&T Directorate/OSTP that have the potential to meet sector CI/KR protection challenges, and provide a description of how this listing will be analyzed to indicate which initiatives have the greatest potential for producing a positive impact;
 - Analyze the gaps between the sector's technology needs and current R&D initiatives from the DHS S&T Directorate/OSTP; and
 - Determine which candidate R&D initiatives are most relevant for the sector and how these will be summarized.
- Ongoing planning, management, and resources.

Appendixes (As appropriate for details in order to keep the text in the main body of the document concise; include implementation actions.)

Appendix 1: Glossary and Acronyms

Appendix 2: Authorities

Appendix 3: Implementation Actions

Appendix 4: (additional appendices as required)

Appendix 5C: State, Territorial, Tribal and Local Government Considerations

This Appendix outlines a basic framework to guide the development of CI/KR protection strategies, plans, and programs in coordination with the NIPP.

State, Territorial, local, and tribal CI/KR protection efforts enhance the implementation of the NIPP and the SSPs by providing a geographical focus and cross-sector coordination. The NIPP recognizes there is not a “one size fits all” approach to CI/KR protection planning at the State and local levels. This appendix provides general guidance that can be tailored to unique geographical characteristics, government organizational structures, and operating environments.

As part of this effort to frame CI/KR protection planning efforts, the NIPP is structured to avoid redundancy between State and local efforts and Federal CI/KR protection. States or localities are encouraged to focus their efforts in ways that leverage Federal resources and address the relevant CI/KR sector’s protection requirements in their particular areas or jurisdictions. To align with the NIPP, State and local CI/KR protection programs should explicitly address six broad categories when describing their CI/KR protection approach:

- CI/KR protection roles and responsibilities;
- Building partnerships and information sharing;
- Implementing the NIPP risk management framework;
- CI/KR data use and protection;
- Leveraging ongoing emergency preparedness activities for CI/KR protection; and
- Integrating Federal CI/KR protection activities.

These categories are in addition to any other descriptions of local CI/KR protection projects and activities that may already exist. State and local entities should treat the material presented under each of the six categories as indications of possible approaches, not explicit requirements.

5C.1 CI/KR Roles and Responsibilities

The NIPP outlines a set of broad responsibilities for State, regional, local, and tribal entities (see Chapter 2). To ensure that CI/KR protection roles are performed, State, regional, local, and tribal CI/KR protection plans (or elements addressing CI/KR in State or local homeland security plans or strategies) should describe how each jurisdiction intends to implement these roles. In particular, jurisdictions should consider and describe in their plans the following:

- Which, if any, existing offices or organizations in the jurisdiction currently perform a role or responsibility outlined in the NIPP or any SSP that is relevant to the jurisdiction;
- Whether gaps exist between the jurisdiction’s current operations and roles outlined in the NIPP or in an SSP and how the gaps will be addressed;

- Whether roles not currently performed by other offices or organizations can be consolidated or assigned to an appropriate jurisdictional entity;
- Whether any roles need to be modified to accommodate the unique operating attributes of the jurisdiction;
- Whether there are additional roles and responsibilities based on the unique features of the jurisdiction that need to be identified and assigned;
- How CI/KR protection roles assigned to disparate offices or organizations within the jurisdiction can be coordinated through one office or a single reporting mechanism;
- How the jurisdiction will maintain operational awareness of the performance of CI/KR protection roles assigned to different offices, agencies, or localities; and
- How the jurisdiction will coordinate its CI/KR protection roles and responsibilities with other jurisdictions and the Federal government.

5C.2 Building Partnerships and Information Sharing

Effective CI/KR protection requires the development of partnerships, collaboration, and information sharing between government and private sector owners and operators. This includes maintaining awareness of CI/KR owner and operator concerns, disseminating relevant information to owners and operators, and maintaining processes for rapid response and decision making in the event of a threat or incident involving the jurisdiction's infrastructure. To address partnership building, networking, and information sharing, State and local entities should determine whether the appropriate mechanisms for sharing information and networking with security partners are in place. If mechanisms are not established, State and local entities should identify means for better coordinating and sharing information with security partners. Options to be considered and described in State, regional, local, and tribal CI/KR protection plans can include, but are not limited to:

- Ensuring collaboration with other government entities and the private sector using a process based on the partnership model outlined under the NIPP or an abbreviated form of the model addressing just those sectors that are most relevant to the jurisdiction;
- Instituting specific information-sharing networks, such as an information-sharing portal, for security partners in the jurisdiction. These types of networks will allow owners and operators and regional governmental entities to share best practices, provide a better understanding of sector and cross-sector needs, and inform collective decision making on how best to utilize resources;
- Developing standing committees and work groups to discuss relevant CI/KR protection issues;
- Developing a regular newsletter or similar communications tool for CI/KR owners and operators on relevant CI/KR protection issues and coordination with the jurisdiction; and
- Participating in existing sector-wide and national information-sharing networks, including those offered by trade associations, Information Sharing and Analysis Centers (ISACs), Sector Coordinating Councils (SCCs), and threat warning and alert notification systems.

The information-sharing approach for a given jurisdiction will vary based on CI/KR ownership, number of relevant CI/KR sectors represented in the jurisdiction, and the extent to which existing mechanisms can be leveraged. The options presented above are merely a description of some available mechanisms that jurisdictions may consider as they develop the organization of their programs and document their processes in a CI/KR protection plan.

5C.3 Implementing the Risk Management Framework

The NIPP risk management framework described in Chapter 3 provides a useful model for State, regional, local, and tribal jurisdictions to use in addressing CI/KR protection within the given jurisdiction. The process provides a risk-based approach that can help State and local entities to identify, prioritize, and protect CI/KR assets and systems within their jurisdictions that, while critical to their operations and their populations, may not be deemed critical at the national level. This process also allows State and local jurisdictions to enhance coordination with DHS and the SSAs in developing and implementing CI/KR protection programs. The following should be considered when developing CI/KR protection programs:

- What are the jurisdiction's goals and objectives for CI/KR protection? How do these goals relate to those of the NIPP and the SSPs that are relevant to the jurisdiction?
- What are the CI/KR assets within the jurisdiction or that impact the jurisdiction? Are there interstate or international dependencies or interdependencies? Are any of the assets or systems within the jurisdiction deemed to be nationally critical by DHS?
- Are Risk Assessments for CI/KR within the State being conducted or planned by DHS, SSAs, or owners and operators in accordance with the processes outlined in the NIPP? Is there a need for the jurisdiction to conduct additional or supplemental risk assessments? Do the methodologies for conducting risk assessments address the baseline criteria outlined in Chapter 3?
- What are the CI/KR protection priorities within the State? How do these priorities correlate with the national priorities established by DHS? How do these priorities correlate with the ongoing CI/KR protection priorities established for each sector at the national level?
- What actions or initiatives are being taken within the jurisdiction to address CI/KR protection? How do these relate to the national effort?
- What types of metrics will be used to measure the progress of CI/KR protection efforts?

5C.4 CI/KR Data Use and Protection

States and other jurisdictions may employ a variety of means to collect CI/KR data or respond to CI/KR data requests. State, regional, local, and tribal plans should outline how the jurisdiction has organized itself to address CI/KR data use and protection. The following issues should be considered in developing the CI/KR protection plan:

- Will the jurisdiction maintain a comprehensive database of critical infrastructures in the State, region, or locality? How will the jurisdiction collect such information?
- Will data collection mechanisms be compatible and interoperable with the National Asset Database (NADB) to improve the ease of data sharing?

- How will the jurisdiction ensure that it is maintaining current information?
- Will data requests from the Federal government for CI/KR data be filtered to the owners and operators for responses or will the State or local government respond on their behalf?
- Are there local legal authorities and policy directives related to data collection? Are these authorities adequate? If not, how will the jurisdiction address these issues?

5C.5 Leveraging Ongoing Emergency Preparedness Activities for CI/KR Protection

The emergency management capabilities of each State and local jurisdiction are an important component of improving overall CI/KR protection. States and localities should look to existing programs and leverage ways in which CI/KR protection can be integrated into ongoing activities. Areas to be considered when drafting a CI/KR protection plan include:

- Does the State exercise program account for CI/KR protection? If not, how will the State or locality incorporate CI/KR protection exercise scenarios to increase the level of preparedness?
- How do CI/KR protection efforts relate to initiatives outlined in the jurisdiction's Hazard Mitigation plan? How do various hazard modeling or ongoing mitigation efforts relate to the CI/KR protection initiatives?
- How will the jurisdiction share best practices, reports, or other output from emergency preparedness activities with CI/KR owners and operators?
- Have CI/KR owners and operators been invited to participate in exercise events and are CI/KR owners and operators linked to existing warning or response systems?
- What existing education and outreach programs can be leveraged to share information with security partners regarding CI/KR protection?
- Are there other outreach or emergency management programs that should include a CI/KR component?

5C.6 Integrating Federal CI/KR Protection Activities

State and local responsibilities for implementing the NIPP do not require these entities to establish methodologies and criteria or otherwise duplicate the efforts of the SSAs and DHS. Rather, it is expected that these parties will build on the Federal efforts to the maximum extent possible. Each State and locality should consider the adequacy of DHS and SSA guidance and resources for their local situation. For example:

- Are the existing criteria for consequences inclusive of levels of consequences that are of concern to the State or locality or should the jurisdiction's criteria be expanded to include additional local assets?
- Are the self-assessment tools developed by DHS and the SSAs sufficient or do these tools need additional tailoring to reflect local conditions?

- 1 • Are there additional best practices that should be shared among security partners?
- 2 • Are there additional authorities that need to be documented?

Appendix 5D: Recommended Homeland Security Practices for Use by the Private Sector

This appendix provides a summary of practices that may be adopted by private sector owners and operators to improve the efficiency and effectiveness of their CI/KR protective measures. The recommendations are based on best practices currently in use by various sectors and groups. The NIPP encourages private sector owners and operators to adopt and implement those practices that are appropriate and applicable at the specific sector enterprise and individual organization levels:

- **Asset Identification:**

- Implement the NIPP framework for the assets under their control; and
- Provide CI/KR-related data to DHS to facilitate national protection program implementation.

- **Risk/Vulnerability:**

- Conduct appropriate risk and vulnerability assessment activities using tools or methods that are rigorous, well-documented, and based on accepted practices in industry or government;
- Implement measures to reduce risk and mitigate deficiencies and vulnerabilities in the physical, cyber, and human security controls;
- Maintain the tools, capabilities, and protocols to provide an appropriate level of monitoring of the facility and its immediate surroundings to detect possible insider and external threats;
- Develop and implement personnel screening programs for personnel working in sensitive positions; and
- Manage the security of computer systems while maintaining awareness of vulnerabilities and consequences to ensure that systems are not used to enable attacks against CI/KR.

- **Information Sharing:**

- Connect with, and participate in, the appropriate national, regional, State, local, and sector information-sharing mechanisms (e.g., Homeland Security Information Network — Critical Sector (HSIN-CS) or the sector Information Sharing and Analysis Center (ISAC));
- Develop and maintain working relationships with local (and, as appropriate, Federal, State, Territorial, and tribal) law enforcement and first-responder organizations relevant to the company's facilities to promote communication and cooperation related to prevention, remediation, and response to a natural disaster or terrorist event;
- Provide appropriate information on threats, assets, and vulnerabilities to appropriate government authorities when relevant to the government's necessary roles;
- Share threat and other appropriate information with other owners and operators;
- Participate in NIPP Sector Coordinating Council activities;
- Participate in, share information with, and support State and local CI/KR protection programs, including participating with Local Emergency Planning Committees;

- Collaborate with infrastructure owners and operators on issues of mutual concern; and
- Use appropriate measures to safeguard information that would pose a threat in the wrong hands.
- Maintain open and effective communications regarding security measures and issues, as appropriate, with employees, suppliers, customers, government officials, and others.
- **Planning and Awareness:**
 - Develop and exercise appropriate Emergency Response and Business Continuity-of-Operation Plans;
 - Participate in exercises and other activities to enhance individual and sector preparedness;
 - Demonstrate a robust governance capability through its commitment to security and resiliency across the entire company;
 - Develop a Mitigation Plan;
 - Develop and communicate an acceptable plan and protocol for each of the levels of the Homeland Security Advisory System. These plans and protocols are additive so that as the threat level increases for company facilities, the company can quickly implement its plans to enhance the physical security or cybersecurity measures in operation at those facilities;
 - Develop, implement, and exercise appropriate Emergency Response, Business Continuity, and Disaster Recovery Plans to allow the business to survive and respond to a major natural disaster or terrorist event. These plans should provide for physical displacement of the business and all associated human and technology infrastructure for the short term (less than one month) and long term (more than 1 month);
 - Document the key elements of security programs, actions, and periodic reviews as part of a commitment to sustain a consistent, reliable, and comprehensive program over time;
 - Enhance security awareness and capabilities through periodic training, drills, and guidance that involve all employees annually to some extent and, when appropriate, involve others such as emergency response agencies;
 - Consider periodic audits to measure the effectiveness of its planned physical security and cybersecurity measures. These audits and verifications are reported directly to the Chief Executive Officer or the Chief Executive's designee for review and action;
 - Promote emergency response training such as the Community Emergency Response Team training offered by the U.S. Citizen Corps,¹⁵ for employees; and
 - Consider including programs for developing highly secure and trustworthy operating systems in near-term R&D priorities.

¹⁵ U.S. Citizen Corps is a Web-based service for citizens to support their general awareness and preparedness (www.CitizenCorps.gov).

Appendix 6A: Research and Development to Improve CI/KR Protection Capabilities

This appendix provides additional detail on R&D programs and initiatives supporting the NIPP. It includes details of R&D planning and programs undertaken in three areas: (1) those conducted under the National Critical Infrastructure Protection Research and Development Plan (NCIP R&D Plan), (2) those conducted by the SSAs and other agencies in support of requirements set forth in the President's Physical and Cybersecurity CI/KR Protection Strategies, and (3) those classified as Technology Pilot Programs, which develop technology-based solutions using more mature technology.

6A.1 The National Critical Infrastructure Protection R&D Plan

As directed by HSPD-7, the Secretary of Homeland Security works with Director of the Office of Science and Technology Policy (OSTP), Executive Office of the President (EOP), to develop the annual NCIP R&D Plan.

The NCIP R&D Plan uses the three-step approach described below to direct the development of CI/KR protection-related technologies to meet existing and future requirements:

Step 1: Identify CI/KR Protection R&D Strategic Goals and Objectives

The NCIP R&D planning process identifies three long-term strategic goals and provides direction to the R&D community through a prioritized CI/KR protection agenda:

- **A common operating picture architecture** that will integrate infrastructure monitoring and support systems with data collection, processing, analysis, modeling, and simulation, including interdependencies and visualization capabilities to provide real-time analysis and reports on the status and security of the country's CI/KR;
- **A next-generation Internet architecture** with "designed-in security" that is more secure than the existing Internet. The architecture will incorporate security and protection measures at all levels from the basic hardware components through all layers of software as an explicit design feature of this new network rather than adding it later as a post-development patch; and
- **Resilient, self-diagnosing, self-healing systems** that if attacked or damaged can manage or contain the extent of the damage, continue to provide critical services, and adapt and self-heal damaged areas.

Step 2: Identify CI/KR Protection R&D Themes

Science and technology needs for CI/KR protection programs fall into nine topical themes, or R&D areas, that cut across all CI/KR sectors:

- **Detection and Sensors Systems:** Selection, placement, and integration of systems to detect weapons of mass destruction (WMD) intrusion, small arms, intent, humans (actors and victims), and disease outbreak. The research plans for certain sensors and detectors reside within several R&D communities, specifically for chemical, biological, radiological, nuclear and explosive agents. The

standards community also has a role in fostering interoperable sensor systems and in establishing performance specifications.

- **Protection and Prevention Systems:** Devices, methods, and processes that prevent damage or destruction of CI/KR and their interdependencies. This theme involves layers of defensive measures that deter attackers, prevent entry, inhibit the use of weapons, and harden infrastructures.
- **Entry and Access Portals:** Devices, systems, and methods that control access to CI/KR. The types of portals include physical entryways and communications nodes. The objects of interest passing through portals include people, vehicles, goods, cargo and freight, electronic information, and communications. The enabling technologies include full life-cycle identity management, including biometric identification and automated identification strong authentication methods such as biometrics, radio frequency tags, sensor data, and x-ray interrogation systems.
- **Insider Threat Detection:** Profiling, detection, anticipation, and monitoring of activities of trusted persons or automated entities with access to a critical asset, whether central or distributed. This theme focuses on detecting malicious intent, monitoring activities to identify anomalies and early indicators, and prevention and protection through real-time auditing of systems and layered measures to prevent inappropriate actions.
- **Analysis and Decision Support Systems:** Modeling, simulation and analysis, and decision support tools to analyze the complex systems and situations found in terrorist attack scenarios, including dependencies and interdependencies among sectors. This theme is of ubiquitous importance across sectors because CI/KR assets are highly interdependent. Systems to be developed include risk-based prioritization and investment strategy aids; vulnerability assessment tools; modeling and simulation of sector operations, interconnectivity, and the consequences of attacks; and response planning tools to simulate scenarios and evaluate candidate responses.
- **Response, Recovery, and Reconstitution Tools:** Systems, devices, and processes that support first-responders and those building temporary and permanent replacements of damaged infrastructure, and the planning systems for all such efforts. Associated technologies include equipment to detect victims and assess safety hazards, simulation tools for response planning and training, and self-recovery design for cyber systems.
- **Emerging Threats and Vulnerabilities Analysis Aids:** Methods and processes that enable early discovery of emerging threats and vulnerabilities or the potential of adversaries to present new threats. Many emerging physical threats relate to changes in the lethality, detectability, or resistance to countermeasures of WMD agents. New cyber threats include those with the capability to attack a wide range of networks, and new health threats include the emergence of infectious diseases, such as pandemic flu.
- **Advanced Infrastructure Architectures:** Use of new technology and associated designs that address current and future infrastructure needs with replacements that are inherently more secure (e.g., Internet contingency and Supervisory Control and Data Acquisition (SCADA) system security). Greater inherent security can rely on automatic responses to attacks, self-healing features, and co-design of physical and cyber components that can prevent, respond to, or recover from attacks more quickly than current systems. Such improvements can have important dual-use benefits, with systems better able to respond to minor but frequent accidental events that degrade performance.

- **Human and Social Issues:** Research into behavioral issues related to victim response and infrastructure operator actions to enhance understanding and decision making during a terrorist event. The focus areas for this theme include coordination among government and private sectors, user-centered designs, the resiliency of commercial enterprises and the economy, and risk communication and management.

Step 3: Establish the NCIP R&D Technology Roadmap

The final step of the planning process involves the development of the NCIP R&D Technology Roadmap. Patterned after the technology roadmaps in wide use in U.S. industry, the roadmap provides a way for Federal managers such as DHS, OSTP, Office of Management and Budget (OMB), and the SSAs to coordinate infrastructure protection R&D, and provides a systematic approach to identify current technology investment plans, determine gaps, and outline the timeline for addressing unmet requirements.

6A.2 Other R&D That Supports CI/KR Protection

Other R&D efforts, developed in accordance with requirements set forth in the President's **Physical and Cyber CI/KR Protection Strategies**, that will be used to support CI/KR protection are discussed in this section. These requirements include:

- Ensure compatibility of communications systems with interoperability standards;
- Exploration of methods to authenticate and verify personal identity;
- Coordinating the development of CI/KR protection consensus standards; and
- Improvement of technical surveillance, monitoring, and detection capabilities.

Examples of programs in each of these areas are discussed below to illustrate the potential benefits of such programs to security partners.

6A.2.1 Ensure Compatibility of Communications Systems With Interoperability Standards

SAFECOM, a program in the DHS Science and Technology (S&T) Directorate, serves as the Federal umbrella to promote and coordinate initiatives between State, local, and tribal entities to improve first-responder communications through more effective and efficient interoperable wireless communications. SAFECOM's primary role is to work with Federal agencies and public safety personnel to define requirements and to create standards, models, and solutions to help meet those requirements.

SAFECOM's role in standards development is to:

- Support existing or, where necessary, establish a voluntary consensus process that meets the current security environment, identifies and implements the needs and requirements of public safety, and maximizes flexibility and innovation; and

- Develop near-term tools that can maximize the efficiency of public safety technology, such as recommended models for statewide planning, criteria for creating governing bodies, standard operating procedures, grant guidance, and communications-specific exercise methodologies.

The following are key characteristics of SAFECOM's approach to facilitating the development of national voluntary consensus standards for public safety interoperable communications:

- Implements a practitioner-driven approach;
- Applies a comprehensive framework that utilizes a structured life-cycle approach that employs continuously evolving common grant guidance to assist communities in planning and implementing their interoperability solutions;
- Integrates new and legacy systems using a "system of systems"; and
- Establishes industry and government partnerships.

6A.2.2 Explore Methods to Authenticate and Verify Personal Identity

In coordination with a number of Federal agencies, DHS funds several R&D programs related to authentication and verification of personal identity for the CI/KR workforce. Examples include research into the protection of physical infrastructure by authentication of network users, recommendations from the private security guard industry on legislative measures needed to achieve progress in the area of personnel surety (including enhanced capabilities for background checks on personnel with critical access), and advances in basic research.

6A.2.3 Coordinate Development of CI/KR Protection Consensus Standards

DHS works with the American National Standards Institute and the National Institute of Standards and Technology to establish a Homeland Security Standards Panel that has been coordinating the development of consensus standards among the 280 different standards development organizations. An important product of this work was the standards supporting HSPD-12, which mandates reliable forms of identification issued by the Federal government, as well as the identity-proofing guidance supporting the eAuthentication initiative.

6A.2.4 Improve Technical Surveillance, Monitoring, and Detection Capabilities

Advances in surveillance, monitoring, and detection increase the Nation's ability to find threats in the making rather than responding to an attack after the fact. From an R&D perspective, advanced processing of digital video and other data collection methods is important in providing information to responsible security forces in a way that is reliable, practical, and fast. In cooperation with the United Kingdom, U.S. expertise has been brought to bear on reducing the amount of data that needs to be transmitted by extracting out only that information required for sophisticated analysis. Massive data storage capacity that is small and affordable is also nearing readiness for the market as a result of R&D investments by the government and private sectors. These advances make better use of the data collection capacity readily available, while providing information to security forces in a more actionable, focused manner.

In addition, the integration of biological, chemical, and radiological environmental and public health surveillance monitoring and detection capabilities, coupled with analysis tools, provide additional situational awareness and improves the ability of decision makers to determine appropriate courses of action in a WMD event.

6A.3 Technology Pilot Programs

DHS identifies CI/KR protection needs common to certain types of assets or to geographical areas in the course of conducting site assistance, buffer zone protection visits, and other vulnerability and risk assessments. In some situations, a technological development program is required to create or test the appropriate technological solution, and the DHS S&T Directorate works closely with other relevant security partners to conduct a Technology Pilot Program. If the pilot program is successful, the technological solutions are then implemented in other locations where similar needs exist. The following descriptions of Technology Pilot Programs provide good examples of the capabilities that these programs can offer security partners:

6A.3.1 National Capital Region Rail Security Corridor Pilot Project

This pilot project is designed to meet the needs of local law enforcement, first-responders, and the Federal government while supplementing the existing security measures of freight rail operations in the Washington, D.C., area. This pilot project seeks to address security challenges surrounding rail infrastructure and freight traffic through large cities while maintaining fluid rail operations. The pilot project components include a virtual security fence consisting of approximately 200 high-resolution fixed cameras, the use of radio frequency identification (ID) scanners, and virtual gates for chemical and radiological detection. Data from the fence and the gates will be encrypted and transmitted simultaneously to multiple locations, such as U.S. Capitol Police, U.S. Secret Service, the rail corridor's owner/operator, and other applicable Federal or local agencies.

6A.3.2 Constellation Automated Critical Asset Management System (Constellation/ACAMS)

Constellation/ACAMS, developed through a partnership between DHS and the City and County of Los Angeles, encompasses an automated system, tools, resources, and related training to assist in protecting CI/KR located in major urban areas. Constellation/ACAMS enables planning for, responding to, and recovery from catastrophic incidents. As such, it focuses on the unique requirements and information needs of first-responders. It possesses a complete reporting capability to answer both local and national data calls on critical assets, including information about location, size, key contacts, types of hazardous materials on site, and vulnerability assessments. It also provides for the automatic generation of Buffer Zone Protection Plans and pre-incident operational plans for local police and first-responder use.

6A.3.3 South Florida Coastal Surveillance Prototype Test Bed

The DHS S&T Directorate and the U.S. Coast Guard (USCG) planned and funded the South Florida Coastal Surveillance Prototype Test Bed, a port and coastal surveillance prototype in the Port Everglades, Miami, and Key West areas. The evolutionary prototype provides an initial immediate coastal surveillance capability in a high-priority area that:

- 1 • Offers the means to develop and evaluate concept of operations in a real-world environment;
- 2 • Implements and tests interoperability among DHS and Department of Defense systems and networks
- 3 such as the U.S. Navy/USCG Joint Harbor Operations Center (JHOC);
- 4 • Tests and evaluates systems and operational procedures; and
- 5 • Becomes the design standard for follow-on systems in other areas and integration with wider area
- 6 surveillance systems.