National Infrastructure Protection Plan

Partnering to enhance protection and resiliency

2009

Preface

Michael Chertoff

Risk in the 21st century results from a complex mix of manmade and naturally occurring threats and hazards, including terrorist attacks, accidents, natural disasters, and other emergencies. Within this context, our critical infrastructure and key resources (CIKR) may be directly exposed to the events themselves or indirectly exposed as a result of the dependencies and interdependencies among CIKR.

Within the CIKR protection mission area, national priorities must include preventing catastrophic loss of life and managing cascading, disruptive impacts on the U.S. and global economies across multiple threat scenarios. Achieving this goal requires a strategy that appropriately balances resiliency—a traditional American strength in adverse times—with focused, risk-informed prevention, protection, and preparedness activities so that we can manage and reduce the most serious risks that we face.

These concepts represent the pillars of our National Infrastructure Protection Plan (NIPP) and its 18 supporting Sector-Specific Plans (SSPs). The plans are carried out in practice by an integrated network of Federal departments and agencies, State and local government agencies, private sector entities, and a growing number of regional consortia—all operating together within a largely voluntary CIKR protection framework. This multidimensional public-private sector partnership is the key to success in this inherently complex mission area. Building this partnership under the NIPP has been a major accomplishment to date and has facilitated closer cooperation and a trusted relationship in and across the 18 CIKR sectors. Integrating multi-jurisdictional and multi-sector authorities, capabilities, and resources in a unified but flexible approach that can also be tailored to specific sector and regional risk landscapes and operating environments is the path to successfully enhancing our Nation's CIKR protection.

The 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 CIKR protection initiatives into a single national effort. It sets forth a comprehensive risk management framework and clearly defined roles and responsibilities for

the Department of Homeland Security; Federal Sector-Specific Agencies; and other Federal, State, regional, local, tribal, territorial, and private sector partners implementing the NIPP.

The 2009 NIPP captures the evolution and maturation of the processes and programs first outlined in 2006 and was developed collaboratively with CIKR partners at all levels of government and the private sector. Participation in the implementation of the NIPP provides the government and the private sector with the opportunity to use collective expertise and experience to more clearly define CIKR protection issues and practical solutions and to ensure that existing CIKR protection planning efforts, including business continuity and resiliency planning, are recognized.

I ask for your continued commitment and cooperation in the implementation of both the NIPP and the supporting SSPs so that we can continue to enhance the protection of the Nation's CIKR.

Michael Chertoff

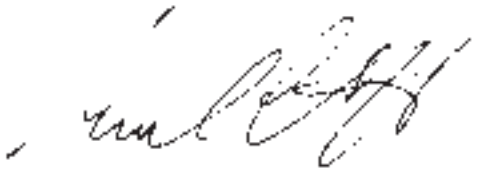


Table of Contents

Preface i

Executive Summary 1

1. Introduction 7

1.1 Purpose 8

1.2 Scope 9

1.3 Applicability 9

1.3.1 Goal 9

1.3.2 The Value Proposition 10

1.4 Threats to the Nation's CIKR 11

1.4.1 The Vulnerability of the U.S. Infrastructure to 21st Century Threats and Hazards 11

1.4.2 The Nature of the Terrorist Adversary 11

1.4.3 All-Hazards and CIKR Protection 11

1.5 Special Considerations 12

1.5.1 The Cyber Dimension 12

1.5.2 International CIKR Protection 12

1.6 Achieving the Goal of the NIPP 13

1.6.1 Understanding and Sharing Information 13

1.6.2 Building Partnerships 13

1.6.3 Implementing a CIKR Risk Management Program 13

1.6.4 Maximizing Efficient Use of Resources for CIKR Protection 14

2. Authorities, Roles, and Responsibilities 15

2.1 Authorities 15

2.2 Roles and Responsibilities 16

2.2.1 Department of Homeland Security 16

2.2.2 Sector-Specific Agencies 18

2.2.3 Other Federal Departments, Agencies, and Offices 20

2.2.4 State, Local, Tribal, and Territorial Governments 21

2.2.5 CIKR Owners and Operators 24

2.2.6 Advisory Councils 25

2.2.7 Academia and Research Centers 25

3. The Strategy: Managing Risk 27
3.1 Set Goals and Objectives 28
3.2 Identify Assets, Systems, and Networks 29
3.2.1 National Infrastructure Inventory 29
3.2.2 Protecting and Accessing Inventory Information 30
3.2.3 SSA Role in Inventory Development and Maintenance 31
3.2.4 State and Local Government Role in Inventory Development and Maintenance 31
3.2.5 Identifying Cyber Infrastructure 32
3.2.6 Identifying Positioning, Navigation, and Timing Services 32
3.3 Assess Risks 32
3.3.1 NIPP Core Criteria for Risk Assessments 33
3.3.2 Risk Scenario Identification 34
3.3.3 Consequence Assessment 34
3.3.4 Vulnerability Assessment 36
3.3.5 Threat Assessment 37
3.3.6 Homeland Infrastructure Threat and Risk Analysis Center 38
3.4 Prioritize 40
3.4.1 The Prioritization Process 40
3.4.2 Tailoring Prioritization Approaches to Sector and Decisionmakers' Needs 41
3.4.3 The Uses of Prioritization 42
3.5 Implement Protective Programs and Resiliency Strategies 42
3.5.1 Risk Management Actions 43
3.5.2 Characteristics of Effective Protective Programs and Resiliency Strategies 43
3.5.3 Risk Management Activities, Initiatives, and Reports 44
3.6 Measure Effectiveness 46
3.6.1 NIPP Metrics Types and Progress Indicators 47
3.6.2 Gathering Performance Information 47
3.6.3 Assessing Performance and Reporting on Progress 48
3.7 Using Metrics and Performance Measurement for Continuous Improvement 48
4. Organizing and Partnering for CIKR Protection 49
4.1 Leadership and Coordination Mechanisms 49
4.1.1 National-Level Coordination 50
4.1.2 Sector Partnership Coordination 50
4.1.3 Regional Coordination and the Partnership Model 53
4.1.4 International CIKR Protection Cooperation 53
4.2 Information Sharing: A Network Approach 56
4.2.1 Supporting the CIKR Protection Mission 57

4.2.2 The CIKR Information-Sharing Environment 60
4.2.3 Federal Intelligence Node 61
4.2.4 Federal Infrastructure Node 62
4.2.5 State, Local, Tribal, Territorial, and Regional Node 62
4.2.6 Private Sector Node 62
4.2.7 DHS Operations Node 63
4.2.8 Other Information-Sharing Nodes 65
4.3 Protection of Sensitive CIKR Information 66
4.3.1 Protected Critical Infrastructure Information Program 66
4.3.2 Other Information Protection Protocols 68
4.4 Privacy and Constitutional Freedoms 69
5. CIKR Protection as Part of the Homeland Security Mission 71
5.1 A Coordinated National Approach to the Homeland Security Mission 71
5.1.1 Legislation 71
5.1.2 Strategies 71
5.1.3 Homeland Security Presidential Directives and National Initiatives 73
5.2 The CIKR Protection Component of the Homeland Security Mission 76
5.3 Relationship of the NIPP and SSPs to Other CIKR Plans and Programs 76
5.3.1 Sector-Specific Plans 76
5.3.2 State, Regional, Local, Tribal, and Territorial CIKR Protection Programs 77
5.3.3 Other Plans or Programs Related to CIKR Protection 77
5.4 CIKR Protection and Incident Management 78
5.4.1 The National Response Framework 78
5.4.2 Transitioning From NIPP Steady-State to Incident Management 78
6. Ensuring an Effective, Efficient Program Over the Long Term 81
6.1 Building National Awareness 81
6.1.1 Education and Training 82
6.1.2 Core Competencies for Implementing CIKR Protection 83
6.1.3 Individual Education and Training 85
6.1.4 Organizational Training and Exercises 86
6.1.5 CIKR Partner Role and Approach 88
6.2 Conducting Research and Development and Using Technology 88
6.2.1 The SAFETY Act 89
6.2.2 National Critical Infrastructure Protection R&D Plan 90
6.2.3 Other R&D That Supports CIKR Protection 91
6.2.4 DHS Science and Technology Strategic Framework 91
6.2.5 Transitioning Requirements Into Reality 91

6.3 Building, Protecting, and Maintaining Databases, Simulations, and Other Tools 92
6.3.1 National CIKR Protection Data Systems 92
6.3.2 Simulation and Modeling 93
6.3.3 Coordination on Databases and Modeling 94
6.4 Continuously Improving the NIPP and the SSPs 94
6.4.1 Management and Coordination 94
6.4.2 Maintenance and Updates 95
7. Providing Resources for the CIKR Protection Program 97
7.1 The Risk-Informed Resource Allocation Process 97
7.1.1 Sector-Specific Agency Reporting to DHS 98
7.1.2 State Government Reporting to DHS 98
7.1.3 State, Local, Tribal, and Territorial Government Coordinating Council Reporting to DHS 99
7.1.4 Regional Consortium Coordinating Council Reporting to DHS 99
7.1.5 Aggregating Submissions to DHS 99
7.2 Federal Resource Prioritization for DHS, the SSAs, and Other Federal Agencies 100
7.2.1 Department of Homeland Security 100
7.2.2 Sector-Specific Agencies 100
7.2.3 Summary of Roles and Responsibilities 101
7.3 Federal Resources for State and Local Government Preparedness 101
7.3.1 Overarching Homeland Security Grant Programs 101
7.3.2 Targeted Infrastructure Protection Programs 102
7.4 Other Federal Grant Programs That Contribute to CIKR Protection 102
7.5 Setting an Agenda in Collaboration with CIKR Protection Partners 103
List of Acronyms and Abbreviations 105
Glossary of Key Terms 109

Appendixes

Appendix 1: Special Considerations 113
Appendix 1A: Cross-Sector Cybersecurity 113
Appendix 1B: International CIKR Protection 125
Appendix 2: Summary of Relevant Statutes, Strategies, and Directives 135
Appendix 3: The Protection Program 147
Appendix 3A: NIPP Core Criteria for Risk Assessments 147
Appendix 3B: Existing CIKR Protection Programs and Initiatives 149
Appendix 3C: Infrastructure Data Warehouse 155
Appendix 4: Existing Coordination Mechanisms 159
Appendix 5: Integrating CIKR Protection as Part of the Homeland Security Mission 163
Appendix 5A: State, Local, Tribal, and Territorial Government Considerations 163
Appendix 5B: Recommended Homeland Security Practices for Use by the Private Sector 167
Appendix 6: S&T Plans, Programs, and Research & Development 171

List of Figures and Tables

Figures

Figure S-1: Protection 2
Figure S-2: NIPP Risk Management Framework 4
Figure 1-1: Protection 7
Figure 3-1: NIPP Risk Management Framework 27
Figure 3-2: NIPP Risk Management Framework: Set Goals and Objectives 29
Figure 3-3: NIPP Risk Management Framework: Identify Assets, Systems, and Networks 30
Figure 3-4: NIPP Risk Management Framework: Assess Risks 33
Figure 3-5: NIPP Risk Management Framework: Prioritize 40
Figure 3-6: NIPP Risk Management Framework: Implement Programs 42
Figure 3-7: NIPP Risk Management Framework: Measure Effectiveness 46
Figure 3-8: NIPP Risk Management Framework: Feedback Loop for Continuous Improvement of CIKR Protection 48
Figure 4-1: Sector Partnership Model 50
Figure 4-2: NIPP Networked Information-Sharing Approach 58
Figure 5-1: National Framework for Homeland Security 72
Figure 6-1: Continuum of CIKR Capability Development 82
Figure 6-2: Developing CIKR Core Competencies 83
Figure 6-3: National Exercise Program Tiers 87
Figure 6-4: The NIPP R&D Requirements Generation Process 92
Figure 7-1: National CIKR Protection Annual Report Process 99
Figure 7-2: National CIKR Protection Annual Report Analysis 100
Figure 7-3: DHS and SSA Roles and Responsibilities in Federal Resource Allocation 101

Tables

Table S-1: Sector-Specific Agencies and Assigned CIKR Sectors 3
Table 2-1: Sector-Specific Agencies and Assigned CIKR Sectors 19
Table 6-1: CIKR Competencwy Areas 84
Table 3C-1: Database Integration 156

Executive Summary

Protecting and ensuring the resiliency of the critical infrastructure and key resources (CIKR) of the United States is essential to the Nation's security, public health and safety, economic vitality, and way of life. Attacks on CIKR 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, manmade, or technological hazards could produce catastrophic losses in terms of human casualties, property destruction, and economic effects, as well as profound damage to public morale and confidence. Attacks using components of the Nation's CIKR as weapons of mass destruction could have even more devastating physical and psychological consequences.

1 Introduction

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

> ***Build a safer, more secure, and more resilient America by preventing, deterring, neutralizing, or mitigating the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit elements of our Nation's CIKR and to strengthen national preparedness, timely response, and rapid recovery of CIKR in the event of an attack, natural disaster, or other emergency.***

The NIPP provides the unifying structure for the integration of existing and future CIKR protection efforts and resiliency strategies into a single national program to achieve this goal. The NIPP framework supports the prioritization of protection and resiliency initiatives and investments across sectors to ensure that government and private sector resources are applied where they offer the most benefit for mitigating risk by lessening vulnerabilities, deterring threats, and minimizing the consequences of terrorist attacks and other manmade and natural disasters. The NIPP risk management framework recognizes and builds on existing public and private sector protective programs and resiliency strategies in order to be cost-effective and to minimize the burden on CIKR owners and operators.

Protection includes actions to mitigate the overall risk to CIKR assets, systems, networks, functions, or their interconnecting links. In the context of the NIPP, this includes actions to deter the threat, mitigate vulnerabilities, or minimize the consequences associated with a terrorist attack or other incident (see figure S-1). Protection can include a wide range of activities, such as improving security protocols, hardening facilities, building resiliency and redundancy, incorporating hazard resistance into facility design, initiating active or passive countermeasures, installing security systems, leveraging "self-healing" technologies, promoting workforce surety programs, implementing cybersecurity measures, training and exercises, business continuity planning, and restoration and recovery actions, among various others.

Achieving the NIPP goal requires actions to address a series of objectives, which include:

- Understanding and sharing information about terrorist threats and other hazards with CIKR partners;
- Building partnerships to share information and implement CIKR protection programs;

Figure S-1: Protection

- Implementing a long-term risk management program; and
- Maximizing the efficient use of resources for CIKR protection, restoration, and recovery.

These objectives require a collaborative partnership among CIKR partners, including: the Federal Government; State, local, tribal, and territorial governments; regional coalitions; the private sector; international entities; and nongovernmental organizations. The NIPP provides the framework that defines a set of flexible processes and mechanisms that these CIKR partners will use to develop and implement the national program to protect CIKR across all sectors over the long term.

2 Authorities, Roles, and Responsibilities

The Homeland Security Act of 2002 provides the basis for Department of Homeland Security (DHS) responsibilities in the protection of the Nation's CIKR. The act assigns DHS the responsibility for developing a comprehensive national plan for securing CIKR 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."

The national approach for CIKR protection is provided through the unifying framework established in Homeland Security Presidential Directive 7 (HSPD-7). This directive establishes the U.S. policy for "enhancing protection of the Nation's CIKR" and mandates a national plan to actuate that policy. In HSPD-7, the President designates the Secretary of Homeland Security as the "principal Federal official to lead CIKR protection efforts among Federal departments and agencies, State and local governments, and the private sector" and assigns responsibility for CIKR sectors to Federal Sector-Specific Agencies (SSAs) (see table S-1). It also provides the criteria for establishing or recognizing additional sectors. In accordance with HSPD-7, the NIPP delineates the roles and responsibilities for partners in carrying out CIKR protection activities while respecting and integrating the authorities, jurisdictions, and prerogatives of these partners.

Primary roles for CIKR partners include:

- **Department of Homeland Security:** Coordinates the Nation's overall CIKR protection efforts and oversees NIPP development, implementation, and integration with national preparedness initiatives.
- **Sector-Specific Agencies:** Implement the NIPP framework and guidance as tailored to the specific characteristics and risk landscapes of each of the CIKR sectors.
- **Other Federal Departments, Agencies, and Offices:** Implement specific CIKR protection roles designated in HSPD-7 or other relevant statutes, executive orders, and policy directives.
- **State, Local, Tribal, and Territorial Governments:** Develop and implement a CIKR protection program, in accordance with the NIPP risk management framework, as a component of their overarching homeland security programs.
- **Regional Partners:** Use partnerships that cross jurisdictional and sector boundaries to address CIKR protection within a defined geographical area.
- **Boards, Commissions, Authorities, Councils, and Other Entities:** Perform regulatory, advisory, policy, or business oversight functions related to various aspects of CIKR operations and protection within and across sectors and jurisdictions.
- **Private Sector Owners and Operators:** Undertake CIKR protection, restoration, coordination, and cooperation activities, and provide advice, recommendations, and subject matter expertise to all levels of government.
- **Homeland Security Advisory Councils:** Provide advice, recommendations, and expertise to the government regarding protection policy and activities.
- **Academia and Research Centers:** Provide CIKR protection subject matter expertise, independent analysis, research and development (R&D), and educational programs.

3 The CIKR Protection Program Strategy: Managing Risk

The cornerstone of the NIPP is its risk analysis and management framework (see figure S-2) that establishes the processes for combining consequence, vulnerability, and threat information to produce assessments of national or sector

Table S-1: Sector-Specific Agencies and Assigned CIKR Sectors

Sector-Specific Agency	Critical Infrastructure and Key Resources Sector
Department of Agriculture[a] Department of Health and Human Services[b]	Agriculture and Food
Department of Defense[c]	Defense Industrial Base
Department of Energy	Energy[d]
Department of Health and Human Services	Healthcare and Public Health
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Water[e]
Department of Homeland Security *Office of Infrastructure Protection*	Chemical Commercial Facilities Critical Manufacturing Dams Emergency Services Nuclear Reactors, Materials, and Waste
Office of Cybersecurity and Communications	Information Technology Communications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration *United States Coast Guard*[f]	Transportation Systems[g]
Immigration and Customs Enforcement, Federal Protective Service	Government Facilities[h]

[a] The Department of Agriculture is responsible for agriculture and food (meat, poultry, and egg products).

[b] The Department of Health and Human Services is responsible for food other than meat, poultry, and egg products.

[c] Nothing in this plan impairs or otherwise affects the authority of the Secretary of Defense over the Department of Defense (DoD), including the chain of command for military forces from the President as Commander in Chief, to the Secretary of Defense, to the commander of military forces, or military command and control procedures.

[d] The Energy Sector includes the production, refining, storage, and distribution of oil, gas, and electric power, except for commercial nuclear power facilities.

[e] The Water Sector includes drinking water and wastewater systems.

[f] The U.S. Coast Guard is the SSA for the maritime transportation mode.

[g] As stated in HSPD-7, the Department of Transportation and the Department of Homeland Security will collaborate on all matters relating to transportation security and transportation infrastructure protection.

[h] The Department of Education is the SSA for the Education Facilities Subsector of the Government Facilities Sector.

risk. The risk management framework is structured to promote continuous improvement to enhance CIKR protection by focusing activities on efforts to: set goals and objectives; identify assets, systems, and networks; assess risk based on consequences, vulnerabilities, and threats; establish priorities based on risk assessments and, increasingly, on return-on-investment for mitigating risk; implement protective programs and resiliency strategies; and measure effectiveness. The results of these processes drive CIKR risk-reduction and management activities. The NIPP risk management framework is tailored to and applied on an asset, system, network, or mission essential function basis, depending on the fundamental characteristics of the individual CIKR sectors. DHS, the SSAs, and other CIKR partners share responsibilities for implementing the risk management framework.

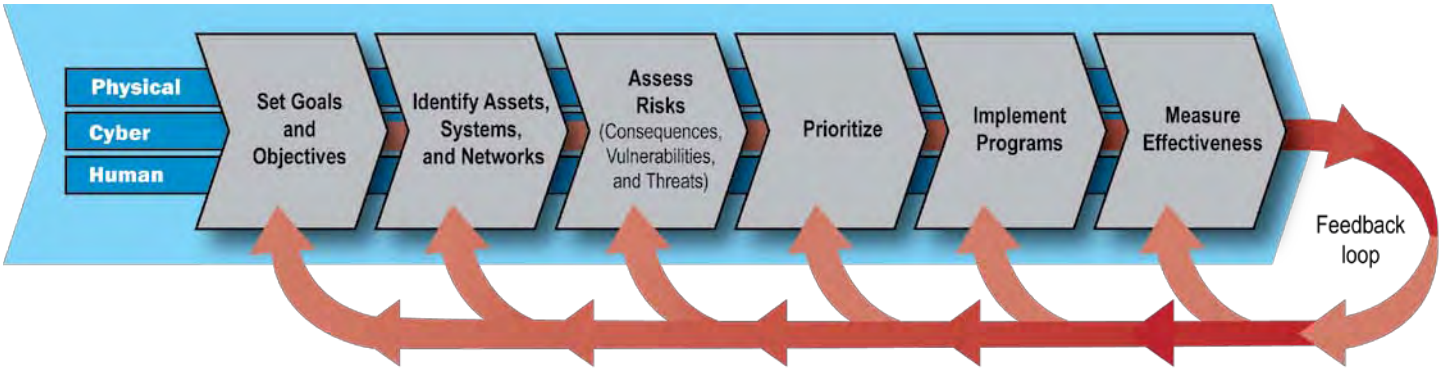
4 Organizing and Partnering for CIKR Protection

The enormity and complexity of the Nation's CIKR, the distributed character of our national protective architecture, and the uncertain nature of the terrorist threat and other manmade or natural disasters make the effective implementation of protection and resiliency efforts a great challenge. To be effective, the NIPP must be implemented using organizational structures and partnerships committed to sharing and protecting the information needed to achieve the NIPP goal and supporting objectives.

The NIPP defines the organizational structures that provide the framework for coordination of CIKR protection efforts at all levels of government, as well as within and across sectors. Sector-specific planning and coordination are addressed through coordinating councils that are established for each sector. Sector Coordinating Councils (SCCs) comprise the representatives of owners and operators, generally from the private sector. Government Coordinating Councils (GCCs) comprise the representatives of the SSAs; other Federal departments and agencies; and State, local, tribal, and territorial governments. These councils create a structure through which representative groups from all levels of government and the private sector can collaborate or share existing approaches to CIKR protection and work together to advance capabilities. Engaging and coordinating with foreign governments and international organizations are also essential to ensuring the protection and resiliency of U.S. CIKR, both at home and abroad. The NIPP provides the mechanisms and processes necessary to enable DHS, the Department of State, the SSAs, and other partners to strengthen international cooperation to support CIKR protection activities and initiatives.

DHS works with cross-sector entities established to promote coordination, communications, and sharing of best practices across CIKR sectors, jurisdictions, or specifically defined geographical areas. Cross-sector issues are challenging to identify and assess comparatively. Interdependency analysis is often so complex that modeling and simulation capabilities must be brought to bear. Cross-sector issues and interdependencies are addressed among the SCCs through the CIKR Cross-Sector Council, which comprises the leadership of each of the SCCs. The Partnership for Critical Infrastructure Security provides this representation with support from the DHS CIKR Executive Secretariat. Cross-sector issues and interdependencies among the GCCs are addressed through the Government Cross-Sector Council, which comprises the NIPP Federal Senior Leadership Council (FSLC) and the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC). Additionally, the Regional Consortium Coordinating Council (RCCC) provides a forum for those with regionally based interests in CIKR protection.

Figure S-2: NIPP Risk Management Framework



Efficient information-sharing and information-protection processes based on mutually beneficial, trusted relationships help ensure implementation of effective, coordinated, and integrated CIKR protection programs and activities. Information sharing enables both government and private sector partners to assess events accurately, formulate risk assessments, and determine appropriate courses of action. The NIPP uses a network approach to information sharing that represents a new model for how CIKR partners share and protect the information needed to analyze risk and make risk-informed decisions. A network approach enables secure, multidirectional information sharing between and across government and industry. This approach provides mechanisms, using information-protection protocols as required, to support the development and sharing of strategic and specific threat assessments, threat warnings, incident reports, all-hazards consequence assessments, risk assessments, and best practices. This information-sharing approach allows CIKR partners to assess risks, identify and prioritize risk management opportunities, allocate resources, conduct risk management activities, and make continuous improvements to the Nation's CIKR protection posture.

NIPP implementation relies on CIKR information provided voluntarily by owners and operators. Much of this is sensitive business or security information that could cause serious damage to private firms, the economy, public safety, or security through unauthorized disclosure or access. The Federal Government has a statutory responsibility to safeguard CIKR protection-related information. DHS and other Federal agencies use a number of programs and procedures, such as the Protected Critical Infrastructure Information (PCII) Program, to ensure that security-related information is properly safeguarded.

The CIKR protection activities defined in the NIPP are guided by legal requirements such as those described in the Privacy Act of 1974 and are designed to achieve both security and protection of civil rights and liberties.

5 CIKR Protection: An Integral Part of the Homeland Security Mission

The NIPP defines the CIKR protection component of the homeland security mission. Implementing CIKR protection requires partnerships, coordination, and collaboration among all levels of government and the private sector. To enable this, the NIPP provides guidance on the structure and content of each sector's CIKR plan, as well as the CIKR protection-related aspects of State and local homeland security plans. This provides a baseline framework that informs the flexible and tailored development, implementation, and updating of Sector-Specific Plans; State and local homeland security strategies; and partner CIKR protection programs and resiliency strategies.

To be effective, the NIPP must complement other plans designed to help prevent, prepare for, protect against, respond to, and recover from terrorist attacks, natural disasters, and other emergencies. Homeland security plans and strategies at the Federal, State, local, tribal, and territorial levels of government address CIKR protection within their respective jurisdictions. Similarly, CIKR owners and operators have responded to the increased threat environment by instituting a range of CIKR protection-related plans and programs, including business continuity and resilience and response measures. Implementation of the NIPP is coordinated among CIKR partners to ensure that it does not result in the creation of duplicative or costly risk management requirements that offer little enhancement of CIKR protection.

The NIPP, the National Preparedness Guidelines (NPG), and the National Response Framework (NRF) together provide a comprehensive, integrated approach to the homeland security mission. The NIPP establishes the overall risk-informed approach that defines the Nation's CIKR protection posture, while the NRF provides the approach for domestic incident management. The NPG sets forth national priorities, doctrine, and roles and responsibilities for building capabilities across the prevention, protection, response, and recovery mission areas. Increases in CIKR protective measures in the context of specific threats or that correspond to the threat conditions established in the Homeland Security Advisory System (HSAS) provide an important bridge between NIPP steady-state protection and the incident management activities under the NRF.

The NRF is implemented to guide overall coordination of domestic incident management activities. NIPP partnerships and processes provide the foundation for the CIKR dimension of the NRF, facilitating threat and incident management across a spectrum of activities, including incident prevention, response, and recovery. The NPG is implemented through the application of target capabilities during the course of assessment, planning, training, exercises, grants, and technical assistance activities. Implementation of the NIPP is both a national preparedness priority and a framework with which to achieve protection capabilities as defined by the NPG.

6 Ensuring an Effective, Efficient Program Over the Long Term

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

- Building national awareness to support the CIKR protection program, related protection investments, and protection activities by ensuring a focused understanding of all hazards and of what is being done to protect and enable the timely restoration of the Nation's CIKR in light of 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 research and development and using technology to improve CIKR protection-related capabilities or to lower the costs of existing capabilities so that CIKR partners can afford to do more with limited budgets;
- Developing, safeguarding, and maintaining data systems and simulations to enable continuously refined risk assessment within and across sectors and to ensure preparedness for incident management; and
- Continuously improving the NIPP and associated plans and programs through ongoing review and revision, as required.

7 Providing Resources for the CIKR Protection Program

Chapter 7 describes an integrated, risk-informed approach used to: establish priorities, determine requirements, and guide resource support for the national CIKR protection program; focus Federal grant assistance to State, local, tribal, and territorial entities; and complement relevant private sector activities. At the Federal level, DHS provides recommendations regarding CIKR protection priorities and requirements to the Executive Office of the President through the National CIKR Protection Annual Report. This report is based on information about priorities, requirements, and related program funding information that is submitted to DHS by the SSA of each sector, the SLTTGCC, and the RCCC as assessed in the context of the National Risk Profile and national priorities. The process for allocating Federal resources through grants to State, local, and tribal governments uses a similar approach. DHS aggregates information regarding State, local, tribal, and territorial CIKR protection priorities and requirements. DHS uses these data to inform the establishment of national priorities for CIKR protection and to help ensure that resources are prioritized for protective programs that have the greatest potential for mitigating risk. This risk-informed approach also includes mechanisms to involve private sector partners in the planning process and supports collaboration among CIKR partners to establish priorities, define requirements, share information, and maximize risk reduction.

1. Introduction

Protecting and ensuring the continuity of the critical infrastructure and key resources (CIKR) of the United States is essential to the Nation's security, public health and safety, economic vitality, and way of life. CIKR includes systems and assets, whether physical or virtual, so vital to the United States that the incapacitation or destruction of such systems and assets would have a debilitating impact on national security, national economic security, public health or safety, or any combination of those matters. Terrorist attacks on our CIKR, as well as other manmade or natural disasters, could significantly disrupt the functioning of government and business alike and produce cascading effects far beyond the affected CIKR and physical location of the incident. Direct and indirect impacts could result in large-scale human casualties, property destruction, economic disruption, and mission failure, and also significantly damage national morale and public confidence. Terrorist attacks using components of the Nation's CIKR as weapons of mass destruction (WMD)[1] could have even more devastating physical, psychological, and economic consequences.

Protecting the Nation's CIKR is essential to making America safer, more secure, and more resilient in the context of terrorist attacks and other natural and manmade hazards. **Protection** includes actions to mitigate the overall risk to CIKR assets, systems, networks, functions, or their interconnecting links resulting from exposure, injury, destruction, incapacitation, or exploitation. In the context of the National Infrastructure Protection Plan (NIPP), this includes actions to deter the threat, mitigate vulnerabilities, or minimize the consequences associated with a terrorist attack or other manmade or natural disaster (see figure 1-1). Protection can include a wide range of activities such as improving security protocols, hardening facilities, building resiliency and redundancy, incorporating hazard resistance into facility design, initiating active or passive countermeasures, installing security systems, leveraging "self-healing" technologies, promoting workforce surety programs, implementing cybersecurity measures, training and exercises, and business continuity planning, among others. The NIPP (June 2006; revised January 2009) and its complementary Sector-Specific Plans (SSPs) (May 2007; to be reissued in 2010) provide a

Figure 1-1: Protection

[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, (v) mine, or (vi) similar device; (2) any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors; (3) any weapon involving a disease organism; or (4) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life (18 U.S.C. 2332a).

consistent, unifying structure for integrating both existing and future CIKR protection efforts. The NIPP also provides the core coordinating processes and mechanisms that enable all levels of government and private sector partners to work together to implement CIKR protection in an effective and efficient manner.

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

Since the NIPP and the SSPs were first released, the processes and programs outlined in those documents have continued to evolve and mature. This update to the NIPP reflects many advances, including:

- The issuance of the SSPs, which followed the release of the NIPP;
- Establishment of Critical Manufacturing as the 18th CIKR sector and the designation of Education as a subsector of Government Facilities;
- Expansion of the sector partnership model to include the geographically focused Regional Consortium Coordinating Council (RCCC);
- CIKR mission integration within State and local fusion centers;
- Evolution of the National Asset Database to the Infrastructure Information Collection System and the Infrastructure Data Warehouse;
- Developments in the programs, approaches, and tools used to implement the NIPP risk management framework;
- Updates on risk methodologies, information-sharing mechanisms, and other CIKR protection programs;
- Inclusion of outcome-focused performance measurement and reporting processes;
- Description of additional Homeland Security Presidential Directives, national strategies, and legislation;
- Release of the Chemical Facility Anti-Terrorism Standards (CFATS), establishing a regulatory framework for those industries that involve the production, use, and storage of high-risk chemicals;
- Discussion of expanded CIKR protection-related education, training, outreach, and exercise programs;
- Evolution from the National Response Plan to the National Response Framework (NRF); and
- Inclusion of further information on research and development (R&D) and modeling, simulation, and analysis processes and initiatives.

Additionally, the revised NIPP integrates the concepts of resiliency and protection, and broadens the focus of NIPP-related programs and activities to an all-hazards environment.

1.1 Purpose

The NIPP provides the framework for the unprecedented cooperation that is needed to develop, implement, and maintain a coordinated national effort to bring together government at all levels, the private sector, nongovernmental organizations, and international partners. The NIPP depends on supporting SSPs for full implementation of this framework within and across CIKR sectors. SSPs are developed by the Federal Sector-Specific Agencies (SSAs) designated in Homeland Security Presidential Directive 7 (HSPD-7) in close collaboration with sector partners.

Together, the NIPP and SSPs provide the mechanisms for: identifying critical assets, systems, and networks, and their associated functions; understanding threats to CIKR; identifying and assessing vulnerabilities and consequences; prioritizing protection initiatives and investments based on costs and benefits so that they are applied where they offer the greatest mitigation of risk; and enhancing information-sharing mechanisms and protection and resiliency within and across CIKR sectors. The NIPP and SSPs will evolve along with changes to the Nation's CIKR and the risk environment, as well as evolving strategies and technologies for protecting against and responding to threats and incidents. Implementation of the NIPP and the SSPs occurs at all levels through actions taken by: Federal agencies; State, regional, local, tribal, and territorial governments and organizations; and individual CIKR owners and operators.

1.2 Scope

The NIPP considers a full range of physical, cyber, and human risk elements within and across sectors. In accordance with the policy direction established in HSPD-7, the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, and the National Strategy to Secure Cyberspace, the NIPP includes a special focus on the unique and potentially catastrophic impact 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. Many of the benefits of enhanced CIKR protection are most sustainable when protective programs and resiliency strategies are designed to address all hazards.

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

1.3 Applicability

The NIPP is applicable to a wide array of public and private sector CIKR partners in different ways. The framework generally is applicable to all partners with CIKR protection responsibilities and includes explicit roles and responsibilities for the Federal Government, including CIKR under the control of independent regulatory agencies, and the legislative, executive, and judicial branches. Federal departments and agencies with specific responsibilities for CIKR protection are required to take actions that are consistent with HSPD-7. The NIPP also provides an organizing structure, guidelines, and recommended activities for other partners to help ensure consistent implementation of the national framework and the most effective use of resources. State,[2] local,[3] tribal, and territorial government partners are required to establish CIKR protection programs that are consistent with the National Preparedness Guidelines and as a condition of eligibility for certain Federal grant programs.

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

1.3.1 Goal

The overarching goal of the NIPP is to:

> ***Build a safer, more secure, and more resilient America by preventing, deterring, neutralizing, or mitigating the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit elements of our Nation's CIKR, and to strengthen national preparedness, timely response, and rapid recovery of CIKR in the event of an attack, natural disaster, or other emergency.***

Achieving this goal requires understanding and sharing information about terrorist threats and other hazards, building partnerships, implementing a long-term risk management program, and maximizing the efficient use of resources. Measuring progress toward achieving the NIPP goal requires that CIKR partners strive toward:

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

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

[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).

1.3.2 The Value Proposition

The public-private partnership called for in the NIPP provides the foundation for effective CIKR protection. Prevention, response, mitigation, and recovery efforts are most efficient and effective when there is the full participation of government and industry partners; the mission suffers (e.g., full benefits are not realized) without the robust participation of a wide array of CIKR partners.

The success of the NIPP partnership depends on articulating the benefits to government and the private sector partners. Industry capabilities that add value to the government include:

- Understanding of CIKR assets, systems, networks, and facilities, and other capabilities through industry ownership and management of a vast majority of CIKR in most sectors;
- Ability to take action to reduce risk and to respond to and recover from incidents;
- Ability to innovate and to provide products, services, and technologies to quickly focus on mission needs; and
- Robust relationships that are useful for sharing and protecting sensitive information regarding threats, vulnerabilities, countermeasures, and best practices.

Although articulating the value proposition to the government typically is easier to achieve, it is often more difficult to articulate the direct benefits of participation for the private sector. In assessing the value proposition for the private sector, there is a clear national interest in ensuring the collective protection and resiliency of the Nation's CIKR. More specific benefits that have been realized during the first few years of the partnership include:

- Participation in both a policy development and risk analysis and management framework that helps focus both corporate and government planning and resource investment;
- Greater information sharing regarding specific threats and hazards enabled by the issuance of security clearances to private sector partners;
- Leveraged application of preparedness guidelines and self-assessment tools within and across sectors so that risks can be managed more effectively and efficiently from the corporate level down to the individual facility level;
- Targeted application of limited resources to the highest risk issues, to include Federal grant funding where appropriate;
- Coordination and planning across multiple agencies for those assets and facilities that are considered to be at the greatest risk;
- Joint R&D and modeling, simulation, and analysis programs;
- Participation in national-level and cross-sector training and exercise programs, as well as the National Incident Management System;
- Access and input into cross-sector interdependency analyses;
- Established informal networks among private sector partners and between the private sector and the various Federal agencies that can be used for all-hazards planning and response; and
- Identification of potential improvements in regulations.

Government can encourage industry to go beyond efforts already justified by their corporate business needs to assist in broad-scale CIKR protection through activities such as:

- Providing owners and operators with timely, accurate, and useful analysis and information on threats to CIKR;
- Ensuring that industry is engaged as early as possible in the development of policies and initiatives related to NIPP implementation;
- Articulating to corporate leaders, through the use of public platforms and private communications, both the business and national security benefits of investing in security measures that exceed their business case;
- Creating an environment that encourages and supports incentives and recognition for companies to voluntarily adopt widely accepted security practices;
- Working with industry to develop and clearly prioritize key missions and enable the protection and/or restoration of related CIKR;
- Providing support for R&D initiatives that is needed to enhance future CIKR protection efforts;
- Providing the resources to enable cross-sector interdependency studies; exercises, symposiums, training sessions, and computer modeling; and otherwise support business continuity planning; and
- Enabling time-sensitive information sharing and restoration and recovery support to priority CIKR facilities and services during emerging threat and incident management situations.

The above examples illustrate some of the ways in which the government can partner with the private sector to add value to industry's ability to assess risk and refine its own business continuity and security plans, as well as to contribute to the security and sustained economic vitality of the Nation.

1.4 Threats to the Nation's CIKR

Presidential guidance and national strategies issued in the aftermath of the September 11, 2001, attacks focused initial CIKR protection efforts on addressing the terrorist threat environment. These new challenges required approaches that focused on intelligence-driven analyses, information sharing, and unprecedented partnerships between the government and the private sector at all levels. The Nation's CIKR owners and operators have decades of experience planning for and responding to natural disasters, industrial accidents, and the deliberate acts of malicious individuals in order to maintain business continuity. However, such plans and preparedness efforts must continue to adapt to a dynamic threat environment and to address vulnerabilities and gaps in CIKR protection in an all-hazards context.

1.4.1 The Vulnerability of the U.S. Infrastructure to 21st Century Threats and Hazards

America is an open, technologically sophisticated, highly interconnected, and complex Nation with a wide array of infrastructure that spans important aspects of the U.S. Government, economy, and society. The vast majority of the CIKR-related assets, systems, and networks are owned and operated by the private sector. However, in sectors such as Water and Government Facilities, the majority of owners and operators are governmental or quasi-governmental entities. The great diversity and redundancy of the Nation's CIKR provide for significant physical and economic resilience in the face of terrorist attacks, natural disasters, or other emergencies, and contribute to the strength of the Nation's economy. However, this vast and diverse aggregation of highly interconnected assets, systems, and networks may also present an attractive array of targets to domestic and international terrorists and magnify greatly the potential for cascading failure in the wake of catastrophic natural or manmade disasters. Improvements in protection and resilience that focus on elements of CIKR that are deemed to be nationally critical can make it more difficult for terrorists to launch destructive attacks, as well as lessen the impact of any attack or other disaster that does occur and provide greater resiliency in response and recovery.

1.4.2 The Nature of the Terrorist Adversary

The number and high profile of international and domestic terrorist attacks and disrupted plots during the last two decades underscore the determination and persistence of terrorist organizations. Terrorists have proven to be relentless, patient, opportunistic, and flexible, learning from experience and modifying tactics and targets to exploit perceived vulnerabilities and avoid observed strengths. Analysis of terrorist goals and motivations points to domestic and international CIKR as potentially prime targets for terrorist attacks. As security measures around more predictable targets increase, terrorists are likely to shift their focus to less protected targets. Enhancing countermeasures to address any one terrorist tactic or target may increase the likelihood that terrorists will shift to another, which underscores the necessity for a balanced, comparative approach that focuses on managing risk commensurately across all sectors and scenarios of concern.

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 CIKR located inside the United States and those located abroad could seriously threaten national security, result in mass casualties, weaken the economy, and damage public morale and confidence.

The NIPP considers a broad range of terrorist objectives, intentions, and capabilities to assess the threat to various components of the Nation's CIKR. Terrorists may contemplate attacks against the Nation's CIKR to achieve direct or indirect effects, or to exploit the infrastructure to cause catastrophic loss of life or economic disruptions.

The NIPP outlines the ways in which the Department of Homeland Security (DHS) and its partners use threat analysis to inform comprehensive risk assessments and risk-mitigation activities. The risk management framework discussed in chapter 3 strikes a balance between ways to mitigate specific threats and general threats. It ensures that the range of risk scenarios considered is broad enough to avoid a "failure of imagination," yet provides a process to enable risk assessment sufficient for the purpose of formulating action plans and programs to enhance resiliency, reduce vulnerability, deter threats, and mitigate potential consequences.

1.4.3 All-Hazards and CIKR Protection

In addition to addressing CIKR protection related to terrorist threats, the NIPP also describes activities relevant to CIKR protection and preparedness in an all-hazards context. The direct impact, disruption, and cascading effects of natural disasters (e.g., Hurricanes Katrina and Rita, the Northridge earthquake, the 2008 Mississippi River floods) and manmade incidents (e.g., the Minneapolis I-35 bridge collapse or the Exxon Valdez oil spill) are documented and underscore the vulnerabilities and interdependencies of the Nation's CIKR.

Many owners and operators, government emergency managers, and first-responders have developed strategies, plans, policies, and procedures to prepare for, mitigate, respond to, and recover from a variety of natural and manmade incidents. The NIPP framework supports these efforts and, additionally, provides an augmented focus on the protection of America's CIKR against terrorist attacks. In fact, the day-to-day public-private coordination structures, information-sharing networks, and risk management frameworks used to implement NIPP steady-state CIKR protection efforts continue to function and provide the CIKR protection dimension for incident management under the National Response Framework (NRF). Likewise, the mitigation and business continuity practices employed to protect against natural hazards and other non-terrorist attacks should support and augment the goals of the NIPP. The NIPP, and the public and private sector partnership that it represents, work in conjunction with other plans and initiatives to provide a strong foundation for preparedness in an all-hazards context.

1.5 Special Considerations

CIKR protection planning involves special consideration for unique cyber elements that support CIKR operations and complex international relationships—two areas of recent focus and attention.

1.5.1 The Cyber Dimension

- The U.S. economy and national security depend greatly and increasingly on the global cyber infrastructure. Cyber infrastructure enables all sectors' functions and services, resulting in a highly interconnected and interdependent global network of CIKR.
- A spectrum of malicious actors routinely conducts attacks against the cyber infrastructure using cyber attack tools. Because of the interconnected nature of the cyber infrastructure, these attacks could spread quickly and have a debilitating effect.
- Cybersecurity includes preventing damage to, unauthorized use of, or exploitation of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. Cybersecurity also includes restoring electronic information and communications systems in the event of a terrorist attack or natural disaster.
- The use of innovative technology and interconnected networks in operations improves productivity and efficiency, but also increases the Nation's vulnerability to cyber threats if cybersecurity is not addressed and integrated appropriately.

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

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

Information Technology (IT) critical functions are sets of processes that produce, provide, and maintain products and services. IT critical functions encompass the full set of processes (e.g., R&D, manufacturing, distribution, upgrades, and maintenance) involved in transforming supply inputs into IT products and services.

- The interconnected and interdependent nature of the Nation's CIKR makes it problematic to address the protection of physical and cyber assets independently.
- The NIPP addresses reducing cyber risk and enhancing cybersecurity in two ways: (1) as a cross-sector cyber element that involves DHS, SSAs and Government Coordinating Councils (GCCs), and private sector owners and operators; and (2) as a major component of the Information Technology Sector's responsibility in partnership with the Communications Sector.

1.5.2 International CIKR Protection

- The NIPP addresses international CIKR protection, including interdependencies and vulnerabilities based on threats (and associated consequences) that originate outside the country or pass through it.
- The Federal Government and the private sector work with foreign governments and international/multinational organizations to enhance the confidentiality, integrity, and availability of cyber infrastructure and products.
- Protection of assets, systems, and networks that operate across or near the borders with Canada and Mexico, or rely on other international aspects to enable critical functionality, requires coordination with and planning and/or sharing resources among neighboring governments at all levels, as well as private sector CIKR owners and operators.
- The Federal Government and private sector corporations have a significant number of facilities located outside the United States that may be considered CIKR.

- Special consideration may be required when CIKR is extensively integrated into an international or global market (e.g., financial services, agriculture, energy, transportation, telecommunications, or information technology) or when a sector relies on inputs that are not within the control of U.S. entities.
- Special consideration is required when government facilities and functions are directly affected by foreign-owned and -operated commercial facilities.
- The Federal Government, working in close coordination and cooperation with the private sector, launched the Critical Foreign Dependencies Initiative in 2007 to identify assets and systems located outside the United States, which, if disrupted or destroyed, would critically affect public health and safety, the economy, or national security. The resulting strategic compendium guides engagement with foreign countries in the CIKR protection mission area.

1.6 Achieving the Goal of the NIPP

Achieving the NIPP goal of building a safer, more secure, and more resilient America requires actions that address the following principal objectives:

- Understanding and sharing information about terrorist threats and other hazards;
- Building partnerships to share information and implement CIKR protection and resiliency programs;
- Implementing a long-term risk management program that includes:
  - Hardening, distributing, diversifying, and otherwise ensuring the resiliency of CIKR against known threats and hazards, as well as other potential contingencies;
  - Developing processes to interdict human threats to prevent potential attacks;
  - Planning for rapid response to CIKR disruptions to limit the impact on public health and safety, the economy, and government functions; and
  - Planning for rapid CIKR recovery for those events that are not preventable; and
- Maximizing the efficient use of resources for CIKR protection.

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

1.6.1 Understanding and Sharing Information

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

- Establishing effective information-sharing processes and protocols among CIKR partners;
- Providing intelligence and information to SSAs and other CIKR sector partners as permitted by law;
- Analyzing, warehousing, and sharing risk assessment data in a secure manner that is consistent with relevant legal requirements and information protection responsibilities;
- Providing protocols for real-time threat and incident reporting, alert, and warning; and
- Providing protocols for the protection of sensitive information.

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

1.6.2 Building Partnerships

Building partnerships represents the foundation of the national CIKR protection effort. These partnerships provide a framework to:

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

Chapters 2 and 4 describe partners' roles and responsibilities related to CIKR protection, as well as specific mechanisms for the governance, coordination, and information sharing necessary to enable effective partnerships.

1.6.3 Implementing a CIKR Risk Management Program

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

- Establish a risk management framework to guide CIKR protection and resiliency programs and activities;
- Take appropriate risk management actions to enhance CIKR protection and resiliency based on all-hazards risk assessments;
- Conduct and update risk assessments, as appropriate, at the asset, system, network, sector, cross-sector, regional, national, and international levels;
- Develop and deploy new technologies to enable more effective and efficient CIKR protection; and
- Provide a system for measurement and improvement of CIKR protection, including:
  - Establishing performance metrics to track the effectiveness of protection programs and resiliency strategies; and
  - Updating the NIPP and SSPs as required.

The NIPP also specifies the processes, initiatives, and milestones necessary to implement an effective long-term CIKR risk management program. Chapter 3 provides details regarding the NIPP risk management framework and the measurement and analysis processes that support its continuous improvement; chapter 6 addresses issues that are important for sustaining and improving CIKR protection over the long term.

1.6.4 Maximizing Efficient Use of Resources for CIKR Protection

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

- Supports prioritization of programs and activities within and across sectors considering sector needs and requirements;
- Informs the annual Federal process regarding planning, programming, and budgeting for national-level CIKR protection;
- Helps align Federal resources with the CIKR protection mission and supports the tracking and accountability of public funds;
- Considers State, local, tribal, and territorial government and private sector issues related to planning, programming, and budgeting;
- Draws on expertise across organizational and national boundaries;
- Shares expertise and speeds implementation of best practices;
- Recognizes the need to build a business case to support further private sector CIKR protection investments; and
- Identifies potential incentives for preparedness and security-related activities where they do not naturally exist in the marketplace.

Chapter 5 explains how a coordinated national approach to the CIKR protection mission supports the efficient application of resources. Efficient use of resources enables the continuous improvement of the technology, databases, data systems, and other approaches used to protect CIKR and manage risk. These processes are detailed in chapter 6. Chapter 7 describes the annual processes that reflect coordination with SSAs and other partners regarding resource prioritization and allocation. Also discussed are processes to target grants and other funding authorities to maximize and focus the use of resources to support national and sector priorities.

More information about the NIPP is available on the Internet at: www.dhs.gov/nipp or by contacting DHS at: nipp@dhs.gov

2. Authorities, Roles, and Responsibilities

Improving the all-hazards protection and resilience of the Nation's CIKR necessitates: a comprehensive, unifying organization; defined roles and responsibilities; and close cooperation across all levels of government and the private sector. Protection authorities, requirements, resources, capabilities, 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 implementing NIPP programs and measuring performance. Hence, successful implementation of the NIPP and the supporting SSPs depends on an effective partnership framework that: fosters integrated, collaborative engagement and interaction; divides responsibilities among diverse Federal, State, regional, local, tribal, territorial, and private sector partners; and helps to efficiently target 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 and GCCs; NIPP partners at all levels of government and in the private sector; CIKR owners and operators; and other partners who share responsibility in protecting the Nation's CIKR. A comprehensive understanding of these roles and responsibilities provides the foundation for an effective and sustainable national CIKR 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, as well as other CIKR protection-related legislation, Executive Orders, Homeland Security Presidential Directives, and national strategies. The National Strategy for Homeland Security established the national CIKR 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] HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection, provided the direction to implement this vision. More detailed information on these and other CIKR protection-related authorities is included in chapter 5 and appendix 2A.

The Homeland Security Act provides the primary authority for the overall homeland security mission and outlines DHS responsibilities in the protection of the Nation's CIKR. It established the DHS mission, including "reducing the Nation's vulnerability to terrorist attacks," major disasters, and other emergencies, and charged the department with evaluating vulnerabilities and ensuring that steps are implemented to protect the high-risk elements of America's CIKR, including food and water systems, agriculture, healthcare systems, emergency services, information technology, communications, banking and finance, energy (electrical, nuclear, gas and oil, and dams), transportation (air, highways, rail, ports, and 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

[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 a local disaster or profoundly damage the Nation's morale or confidence. The Homeland Security Act 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.

national plan for securing CIKR 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 specific legal authorities for both cross-sector and sector-specific CIKR protection and resiliency programs. Examples 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 Maritime Transportation Security Act; the Aviation Transportation Security Act of 2001; the Energy Policy and Conservation Act; the Critical Infrastructure Information Act; the Federal Information Security Management Act; Implementing Recommendations of the 9/11 Commission Act of 2007; and various others.

Many different HSPDs are also relevant to CIKR protection, including, but not limited to:

- HSPD-3, Homeland Security Advisory System
- HSPD-5, Management of Domestic Incidents
- HSPD-8, National Preparedness
- HSPD-9, Defense of the United States Agriculture and Food
- HSPD-10, Biodefense for the 21st Century
- HSPD-19, Combating Terrorist Use of Explosives in the United States
- HSPD-20, National Continuity Policy
- HSPD-22, Domestic Chemical Defense

These separate authorities and directives are tied together as part of the national approach for CIKR 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 CIKR." HSPD-7 establishes a framework for public and private sector partners to identify, prioritize, and protect the Nation's CIKR from terrorist attacks, with an emphasis on protecting against catastrophic health effects and mass casualties. The directive sets forth the roles and responsibilities for: DHS; SSAs; other Federal departments and agencies; State, local, tribal, and territorial governments; regional partners; the private sector; and other CIKR partners. The following sections address the roles and responsibilities under this integrated approach.

2.2 Roles and Responsibilities

Given the fact that terrorist attacks and certain natural or manmade disasters can have a national-level impact, it is incumbent upon the Federal Government to provide leadership and coordination in the CIKR protection mission area.

2.2.1 Department of Homeland Security

Under HSPD-7, DHS is responsible for leading, integrating, and coordinating the overall national effort to enhance CIKR protection, including collaboratively developing the NIPP and supporting SSPs; developing and implementing comprehensive, multi-tiered risk management programs and methodologies; developing cross-sector and cross-jurisdictional protection guidance, guidelines, and protocols; and recommending risk management and performance criteria and metrics within and across sectors. Per HSPD-7, DHS is also a focal point for the security of cyberspace. HSPD-7 establishes a central source for coordinating best practices and supporting protective programs across and within government agencies. In the directive, the President designates 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 infrastructure and key resources." The Secretary of Homeland Security is responsible for addressing the complexities of the Nation's Federal system of government and its multifaceted and interdependent economy, as well as for establishing structures to enhance the close cooperation between the private sector and government at all levels to initiate and sustain an effective CIKR protection program.

In addition to these overarching leadership and cross-sector responsibilities, DHS and its component agencies serve as the SSAs for 11 of the CIKR sectors identified in HSPD-7 or subsequently established using the criteria set forth in HSPD-7: Information Technology; Communications; Transportation Systems; Chemical; Emergency Services; Nuclear Reactors, Materials, and Waste; Postal and Shipping; Dams; Critical Manufacturing; Government Facilities; and Commercial Facilities. Specific SSA responsibilities, as appropriate, are discussed in section 2.2.2. DHS, in the person of the Assistant Secretary for Infrastructure Protection or his/her designee, serves as the co-chair of each of the GCCs with the respective Federal SSA for that sector.

Additional DHS CIKR protection roles and responsibilities include:

- Identifying, prioritizing, and coordinating Federal action in support of the protection of nationally critical assets, systems, and networks, with a particular focus on CIKR that could be exploited to cause catastrophic health effects or mass casualties comparable to those produced by a WMD;
- Coordinating, facilitating, and supporting the overall process for building partnerships and leveraging sector-specific security expertise, relationships, and resources across CIKR sectors, including oversight and support of the sector partnership model described in chapter 4; cooperating with Federal, State, local, tribal, territorial, and regional partners; and collaborating with the Department of State to reach out to foreign governments and international organizations to strengthen the protection of U.S. CIKR;
- Supporting the formation and development of regional partnerships, including promoting new partnerships, enabling information sharing, and sponsoring security clearances;
- Establishing and maintaining a comprehensive, multi-tiered, dynamic information-sharing network designed to provide timely and actionable threat information, assessments, and warnings to public and private sector partners. This responsibility includes protecting sensitive information voluntarily provided by the private sector and facilitating the development of sector-specific and cross-sector information-sharing and analysis systems, mechanisms, and processes;
- Coordinating national efforts for the security of cyber infrastructure, including precursors and indicators of an attack, and understanding those threats in terms of CIKR vulnerabilities;
- Coordinating, facilitating, and supporting comprehensive risk assessment programs for high-risk CIKR, identifying priorities across sectors and jurisdictions, and integrating CIKR protection and resiliency programs with the all-hazards approach to domestic incident management described in HSPD-5;
- Facilitating the sharing of best practices and processes, and risk assessment methodologies and tools across sectors and jurisdictions;
- Ensuring that interagency, sector, and cross-sector coordination and information-sharing mechanisms and resources (e.g., DHS sector specialists) are in place to support CIKR-related incident management operations;
- Sponsoring CIKR protection-related R&D, demonstration projects, and pilot programs;
- Supporting the development and transfer of advanced technologies while leveraging private sector expertise and competencies, including participation in the development of voluntary standards or best practices, as appropriate;
- Promoting national-level CIKR protection education, training, and awareness in cooperation with State, local, tribal, territorial, regional, and private sector partners;
- Identifying and implementing plans and processes for appropriate increases in protective measures that align to all-hazards warnings; specific threats, as appropriate; and each level of the Homeland Security Advisory System (HSAS);
- Providing real-time (24/7) threat and incident reporting;
- Conducting modeling and simulations to analyze sector, cross-sector, and regional dependencies and interdependencies, to include cyber, and sharing the results with CIKR partners, as appropriate;
- Helping inform the annual Federal budget process based on CIKR risk and the potential for reducing risk and need, in coordination with SSAs, GCCs, and other partners;
- Supporting performance measurement for the national CIKR protection program and NIPP implementation process to encourage continuous improvement and providing annual CIKR protection reports to the Executive Office of the President (EOP) and Congress;
- Integrating national efforts for the protection and recovery of critical information systems and the cyber components of physical CIKR, including analysis, warning, information-sharing, and risk management activities and programs;
- Evaluating preparedness for CIKR protection across sectors and jurisdictions;
- Documenting lessons learned from exercises, actual incidents, and pre-disaster mitigation efforts and applying those lessons, where applicable, to CIKR protection efforts;
- Promoting CIKR awareness to provide incentives for participation by CIKR owners and operators;
- Working with the Department of State, SSAs, and other partners to ensure that U.S. CIKR protection efforts are fully coordinated with international partners; and
- Evaluating the need for and coordinating the protection of additional CIKR categories over time, as appropriate.

2.2.2 Sector-Specific Agencies

Recognizing that each CIKR sector possesses its own unique characteristics, operating models, and risk landscapes, HSPD-7 designates Federal Government SSAs for each of the CIKR sectors (see table 2-1). The SSAs are responsible for working with DHS and their respective GCCs to: implement the NIPP sector partnership model and risk management framework; develop protective programs, resiliency strategies, and related requirements; and provide sector-level CIKR protection guidance in line with the overarching guidance established by DHS pursuant to HSPD-7. Working in collaboration with partners, the SSAs are responsible for developing or revising and then submitting SSPs and sector-level performance feedback reports to DHS to enable national cross-sector CIKR protection program assessments.

In accordance with HSPD-7, SSAs are also responsible for collaborating with private sector partners and encouraging the development of appropriate voluntary information-sharing and analysis mechanisms within the sector. This includes encouraging voluntary security-related information sharing, where possible, among private entities within the sector, as well as among public and private entities.

Consistent with existing authorities (including regulatory authorities in some instances), SSAs perform the activities above, as appropriate, and in close cooperation with other sector partners. HSPD-7 requires SSAs to provide an annual report to the Secretary of Homeland Security on their efforts to identify, prioritize, and coordinate CIKR protection and resiliency in their respective sectors. DHS provides guidance and templates that inform reporting on sector CIKR protection priorities, requirements, and resources. The SSA's established annual budget process is the primary mechanism for outlining these sector-specific CIKR protection requirements and related budget projections, to the extent possible, as a component of their annual budget submissions to the Office of Management and Budget (OMB).

Additional SSA responsibilities include:

- Identifying, prioritizing, and coordinating Federal activities in support of CIKR protection and resiliency within the sector, with a particular focus on CIKR that could be exploited to cause catastrophic health effects or mass casualties comparable to those produced by a WMD;
- Managing the overall process for building partnerships and leveraging CIKR security expertise, relationships, and resources within the sector, including sector-level oversight and support of the sector partnership model described in chapter 4;
- Coordinating, facilitating, and supporting comprehensive risk assessment/management programs for high-risk CIKR, identifying protection and resiliency priorities, and incorporating CIKR protection activities as a key component of the all-hazards approach to domestic incident management within the sector;
- Facilitating the sharing of real-time incident notification, as well as CIKR protection best practices and processes, and risk assessment methodologies and tools within the sector;
- Promoting CIKR protection education, training, and awareness within the sector in coordination with State, regional, local, tribal, territorial, and private sector partners;
- Helping inform the annual Federal budget process considering CIKR risk and protection needs in coordination with partners and allocating resources for CIKR protection accordingly;
- Supporting performance measures for CIKR protection and NIPP implementation activities within the sector to enable continuous improvement, and reporting progress and gaps to DHS;
- Contributing to the annual National Critical Infrastructure Protection Research and Development (NCIP R&D) Plan;
- Identifying/recommending appropriate strategies to encourage private sector participation;
- Responding to or otherwise supporting DHS-initiated data calls, as appropriate, to populate the Infrastructure Data Warehouse (IDW), enable national-level risk assessment, and inform the national-level resource allocation;
- Supporting protocols for the Protected Critical Infrastructure Information (PCII) Program, as appropriate;
- Working with DHS, as appropriate, to develop and evaluate sector-specific risk assessment tools;
- Supporting dependency, interdependency, consequence, and other sector analyses, as needed;
- Coordinating with DHS and other NIPP partners to promote CIKR awareness to encourage participation by CIKR owners and operators;
- Coordinating sector-level participation in the National Exercise Program (NEP) (through the NEP Executive Steering Committee representatives), Homeland Security Exercise and Evaluation Program (HSEEP), and other sector-level activities;

Table 2-1: Sector-Specific Agencies and Assigned CIKR Sectors

Sector-Specific Agency	Critical Infrastructure and Key Resources Sector
Department of Agriculture[a] Department of Health and Human Services[b]	Agriculture and Food
Department of Defense[c]	Defense Industrial Base
Department of Energy	Energy[d]
Department of Health and Human Services	Healthcare and Public Health
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Water[e]
Department of Homeland Security *Office of Infrastructure Protection*	Chemical Commercial Facilities Critical Manufacturing Dams Emergency Services Nuclear Reactors, Materials, and Waste
Office of Cybersecurity and Communications	Information Technology Communications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration *United States Coast Guard*[f]	Transportation Systems[g]
Immigration and Customs Enforcement, Federal Protective Service	Government Facilities[h]

[a] The Department of Agriculture is responsible for agriculture and food (meat, poultry, and egg products).

[b] The Department of Health and Human Services is responsible for food other than meat, poultry, and egg products.

[c] Nothing in this plan impairs or otherwise affects the authority of the Secretary of Defense over the Department of Defense (DoD), including the chain of command for military forces from the President as Commander in Chief, to the Secretary of Defense, to the commander of military forces, or military command and control procedures.

[d] The Energy Sector includes the production, refining, storage, and distribution of oil, gas, and electric power, except for commercial nuclear power facilities.

[e] The Water Sector includes drinking water and wastewater systems.

[f] The U.S. Coast Guard is the SSA for the maritime transportation mode.

[g] As stated in HSPD-7, the Department of Transportation and the Department of Homeland Security will collaborate on all matters relating to transportation security and transportation infrastructure protection.

[h] The Department of Education is the SSA for the Education Facilities Subsector of the Government Facilities Sector.

- Assisting sector partners in their efforts to:
  - Organize and conduct protection and continuity-of-operations planning, and elevate awareness and understanding of threats and vulnerabilities to their assets, systems, and networks; and
  - Identify and promote effective sector-specific best practices and methodologies;
- Supporting the identification and implementation of plans and processes within the sector for enhancements in protective measures that align to all-hazards warnings; specific threats, as appropriate; and each level of the HSAS;
- Understanding and mitigating sector-specific cyber risk by developing or encouraging appropriate protective measures, information-sharing mechanisms, and emergency recovery plans for cyber assets, systems, and networks within the sector and interdependent sectors; and
- Coordinating with DHS, the Department of State (DOS), and other appropriate departments and agencies to integrate U.S. CIKR 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 CIKR partners in coordination with DHS and the SSAs. In accordance with HSPD-7, they cooperate with DHS in implementing CIKR 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 supporting identification, prioritization, assessment, and remediation of, and enhancing the protection of, CIKR under their control. Federal departments and agencies that are not designated as SSAs, but that have unique responsibilities, functions, or expertise in a particular CIKR sector (such as GCC members) will:

- Assist in identifying and assessing high-consequence CIKR and enabling protective actions and programs within that sector;
- Support the national goal of enhancing CIKR protection through their role as the regulatory agency for owners and operators represented within a specific sector when so designated by statute; and
- Collaborate with all relevant 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 an important supporting role in developing and implementing the SSPs and 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 CIKR protection. The following section addresses Federal departments, agencies, and commissions specifically identified in HSPD-7. Many other Federal entities have sector-specific or cross-sector authorities and responsibilities that are more appropriately addressed in the SSPs.

- The DOS, in coordination with DHS and the Departments of Justice, Commerce, Defense, and the Treasury, works with foreign governments and international organizations to strengthen U.S. CIKR protection efforts.
- The Department of Justice (DOJ), including the Federal Bureau of Investigation (FBI), acts to reduce terrorist threats and investigates and prosecutes actual or attempted attacks on, sabotage of, or disruptions of CIKR in collaboration with DHS.
- The Department of Commerce (DOC) works with: DHS; the private sector; and research, academic, and government organizations to improve technology for cyber systems and promote other critical infrastructure efforts, including using its authority under the Defense Production Act to ensure the timely availability of materials, services, and facilities to meet homeland security requirements, and to address economic security issues.
- The Department of Transportation (DOT) collaborates with DHS on all matters related to transportation security and transportation infrastructure protection, and is also responsible for operating the National Airspace System. DOT and DHS collaborate on regulating the transportation of hazardous materials by all modes (including pipelines).
- The Nuclear Regulatory Commission (NRC) works with DHS and the Department of Energy (DOE), as appropriate, to ensure the protection of commercial nuclear reactors for generating electric power and non-power nuclear reactors used for research, testing, and training; nuclear materials in medical, industrial, and academic settings and facilities that fabricate nuclear fuel; and the transportation, storage, and disposal of commercial nuclear materials and waste. In addition, the NRC collaborates with DHS on any changes in the protective measures for this sector, as well as the approval of new reactor applications.

- The Intelligence Community, the Department of Defense (DoD), and other appropriate Federal departments, such as the Department of the Interior (DOI) and DOT, have collaborated with DHS to develop and implement a suite of geospatial visualization and analysis tools to map, image, analyze, and sort CIKR data using commercial satellite and airborne systems, as well as associated agency capabilities. DHS works with these Federal departments and agencies to identify and help protect those positioning, navigation, and timing services, such as global positioning systems (GPS), that are critical enablers for CIKR sectors such as Banking and Finance and Communications. DHS and the Intelligence Community also collaborate with other agencies, such as the Environmental Protection Agency, that manage data addressed by geographic information systems.
- The Homeland Security Council ensures the coordination of interagency policy related to physical and cyber CIKR protection based on advice from the Critical Infrastructure Protection Policy Coordination Committee (PCC). This PCC is chaired by a Federal officer or employee designated by the Assistant to the President for Homeland Security.
- The White House Office of Science and Technology Policy coordinates with DHS to further interagency R&D related to CIKR protection.
- The OMB oversees the implementation of government-wide policies, principles, standards, and guidelines for Federal Government computer security programs.

2.2.4 State, Local, Tribal, and Territorial Governments

State, local, tribal, and territorial governments are responsible for implementing the homeland security mission, protecting public safety and welfare, and ensuring the provision of essential services to communities and industries within their jurisdictions. They also play a very important and direct role in enabling CIKR protection and resilience, including CIKR under their control, as well as that owned and operated by other NIPP partners within their jurisdictions. The efforts of these public entities are critical to the effective implementation of the NIPP, SSPs, and various jurisdictionally focused protection and resiliency plans. They are equally critical in terms of enabling time-sensitive, post-event CIKR response and recovery activities.

CIKR partners at all levels of government have developed homeland security strategies that align with and support the priorities established in the National Preparedness Guidelines. With the inclusion of NIPP implementation as one of these national priorities, CIKR protection programs form an essential component of State, local, tribal, and territorial homeland security strategies, particularly with regard to establishing funding priorities and informing security investment decisions. To permit effective NIPP implementation and performance measurement at each jurisdictional level, these protection programs should reference all core elements of the NIPP framework, where appropriate, including key cross-jurisdictional security and information-sharing linkages, as well as specific CIKR protection programs focused on risk management. These programs play a primary role in the identification and protection of CIKR regionally and locally and also support DHS and SSA efforts to identify, ensure connectivity with, and enable the protection of CIKR of national-level criticality within the jurisdiction.

2.2.4.1 State and Territorial Governments

State (and territorial, where applicable) governments are responsible for establishing partnerships, facilitating coordinated information sharing, and enabling planning and preparedness for CIKR protection within their jurisdictions. They serve as crucial coordination hubs, bringing together prevention, protection, response, and recovery authorities; capabilities; and resources among local jurisdictions, across sectors, and between regional entities. States and territories also act as conduits for requests for Federal assistance when the threat or incident situation exceeds the capabilities of public and private sector partners at lower jurisdictional levels. States receive CIKR information from the Federal Government to support national and State CIKR protection and resiliency programs.

State and territorial governments shall develop and implement State or territory-wide CIKR protection programs that reflect the full range of NIPP-related activities. State and territorial programs should address all relevant aspects of CIKR protection, leverage support from homeland security assistance programs that apply across the homeland security mission area, and reflect priority activities in their strategies to ensure that resources are effectively allocated. Effective statewide and regional CIKR protection efforts should be integrated into the overarching homeland security program framework at the State or territory level to ensure that prevention, protection, response, and recovery efforts are synchronized and mutually supportive. CIKR protection at the State or territory level must cut across all sectors present within the State or territory and support national, State, and local priorities. The program also should explicitly address unique geographical issues, including transborder concerns, as well as interdependencies among sectors and jurisdictions within those geographical boundaries.

Specific CIKR protection-related activities at the State and territorial level include, but are not limited to:

- Acting as a focal point for and promoting the coordination of protective and emergency response activities, preparedness programs, and resource support among local jurisdictions, regional organizations, and private sector partners;
- Developing a consistent approach to CIKR identification, risk determination, mitigation planning, and prioritized security investment, and exercising preparedness among all relevant stakeholders within their jurisdictions;
- Identifying, implementing, and monitoring a risk management plan and taking corrective actions, as appropriate;
- Participating in significant national, regional, and local awareness programs to encourage appropriate management and security of cyber systems;
- Acting as conduits for requests for Federal assistance when the threat or current situation exceeds the capabilities of State and local jurisdictions and the private entities resident within them;
- Facilitating the exchange of security information, including threat assessments and other analyses, attack indications and warnings, and advisories, within and across jurisdictions and sectors therein;
- Participating in the NIPP sector partnership model, including: sector-specific GCCs; the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC); SCCs; and other CIKR governance and planning efforts relevant to the given jurisdiction;
- Ensuring that funding priorities are addressed and that resources are allocated efficiently and effectively to achieve the CIKR protection mission in accordance with relevant plans and strategies;
- Sharing information on CIKR deemed to be critical from national, State, regional, local, tribal, and/or territorial perspectives to enable prioritized protection and restoration of critical public services, facilities, utilities, and functions within the jurisdiction;
- Addressing unique geographical issues, including transborder concerns, dependencies, and interdependencies among the sectors within the jurisdiction;
- Identifying and implementing plans and processes for increasing protective measures that align to all-hazards warnings; specific threats, as appropriate; and each level of the HSAS;
- Documenting lessons learned from pre-disaster mitigation efforts, exercises, and actual incidents, and applying that learning, where applicable, to the CIKR context;
- Coordinating with NIPP partners to promote CIKR awareness to motivate participation by CIKR owners and operators;
- Providing response and protection, as appropriate, where there are gaps and where local entities lack the resources needed to address those gaps;
- Identifying and communicating the requirements for CIKR-related R&D to DHS; and
- Providing information, as part of the grants process and/or homeland security strategy updates, regarding State priorities, requirements, and CIKR-related funding needs.

2.2.4.2 Regional Organizations

Regional 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 CIKR protection.

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 partners in implementing NIPP-related CIKR risk assessment and protection activities;
- Facilitate education and awareness of CIKR protection efforts occurring within their geographical areas;
- Participate in regional exercise and training programs, including a focus on CIKR protection collaboration across jurisdictional and sector boundaries;
- Support threat-initiated and ongoing operations-based activities to enhance protection and preparedness, as well as to support mitigation, response, and recovery;
- Work with State, local, tribal, territorial, and international governments and the private sector, as appropriate, to evaluate regional and cross-sector CIKR interdependencies, including cyber considerations;

- Conduct the appropriate regional planning efforts and undertake appropriate partnership agreements to enable regional CIKR protection activities and enhanced response to emergencies;
- Facilitate information sharing and data collection between and among regional initiative members and external partners;
- Share information on progress and CIKR protection requirements with DHS, the SSAs, State and local governments, and other CIKR partners, as appropriate; and
- Participate in the NIPP sector partnership model, as appropriate.

2.2.4.3 Local Governments

Local governments represent the front lines for homeland security and, more specifically, CIKR protection and implementation of the NIPP partnership model. They provide critical public services and functions in conjunction with private sector owners and operators. In some sectors, local governmental entities own and operate CIKR such as water, stormwater, and electric utilities. Most disruptions or malevolent acts that affect CIKR begin and end as local situations. Local authorities typically shoulder the weight of initial prevention, response, and recovery operations until coordinated support from other sources becomes available, regardless of who owns or operates the affected asset, system, or network. As a result, local governments are critical partners under the NIPP framework. They drive emergency preparedness, as well as local participation in NIPP and SSP implementation across a variety of jurisdictional partners, including government agencies, owners and operators, and private citizens in the communities that they serve.

CIKR protection focus at the local level should include, but is not limited to:

- 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 consistent approach at the local level to CIKR identification, risk determination, mitigation planning, and prioritized security investment, and exercising preparedness among all relevant partners within the jurisdiction;
- Identifying, implementing, and monitoring a risk management plan, and taking corrective actions, as appropriate;
- Participating in significant national, State, local, and regional education and awareness programs to encourage appropriate management and security of cyber systems;
- Facilitating the exchange of security information, including threat assessments, attack indications and warnings, and advisories, among partners within the jurisdiction;
- Participating in the NIPP sector partnership model, including GCCs, SCCs, SLTTGCC, and other CIKR structures relevant to the given jurisdiction;
- Ensuring that funding priorities are addressed and that resources are allocated efficiently and effectively to achieve the CIKR protection mission in accordance with relevant plans and strategies;
- Establishing continuity plans and programs that facilitate the performance of critical functions during an emergency or until normal operations can be resumed;
- Sharing with partners, as appropriate, CIKR information deemed to be 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 transborder concerns, dependencies, and interdependencies among agencies and enterprises within the jurisdiction;
- Identifying and implementing plans and processes for step-ups in protective measures that align to all-hazards warnings; specific threats, as appropriate; and each level of the HSAS;
- Documenting lessons learned from pre-disaster mitigation efforts, exercises, and actual incidents, and applying that learning, where applicable, to the CIKR protection context; and
- Conducting CIKR protection public awareness activities.

2.2.4.4 Tribal Governments

Tribal government roles and responsibilities regarding CIKR protection generally mirror those of State and local governments as detailed above. Tribal governments are accountable for the public health, welfare, and safety of tribal members, as well as the protection of CIKR and the continuity of essential services under their jurisdiction. Under the NIPP partnership model, tribal governments shall ensure coordination with Federal, State, local, and international 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, and protective program investments and initiatives.

2.2.4.5 Boards, Commissions, Authorities, Councils, and Other Entities

An array of boards, commissions, authorities, councils, and other entities at the State, local, tribal, and regional levels perform regulatory, advisory, policy, or business oversight functions related to various aspects of CIKR operations and protection within and across sectors and jurisdictions. Some of these entities are established through State- or local-level executive or legislative mandates with elected, appointed, or voluntary membership. These groups include, but are not limited to, transportation authorities, public utility commissions, water and sewer boards, park commissions, housing authorities, public health agencies, and many others. These entities may serve as the equivalents of SSAs within a State and contribute expertise, assist with regulatory authorities, or help facilitate investment decisions related to CIKR protection efforts within a given jurisdiction or geographical region.

2.2.5 CIKR Owners and Operators

Owners and operators generally develop and implement the protective programs and resiliency strategies for the CIKR under their control. CIKR are owned by both the public and private sector; however, the majority of CIKR is owned by the private sector. Owners and operators take 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-business and emergency management plans, building increased resiliency and redundancy into business processes and systems, protecting facilities against physical and cyber attacks, reducing the vulnerability to natural disasters, guarding against insider threats, and increasing coordination with external organizations to avoid or minimize the impact on surrounding communities or other industry partners.

For many private sector enterprises, the level of investment in security reflects risk-versus-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 within resource constraints. In the context of the first factor, the Federal Government is uniquely positioned to help inform critical security investment decisions and operational planning. For example, owners and operators generally look to the government as a source of security-related best practices and for attack or natural hazard indications, warnings, and threat assessments. In relation to the second factor, owners and operators also generally rely on governmental entities to address risks outside of their property or in situations in which the current threat exceeds an enterprise's capability to protect itself or requires an unreasonable level of additional investment to mitigate risk. In this situation, public and private sector partners at all levels must collaborate to address the protection of national-level CIKR, provide timely warnings, and promote an environment in which CIKR owners and operators can better carry out their specific protection responsibilities. Additionally, CIKR owners and operators may be required to invest in security as a result of Federal, State, and/or local regulations.

The CIKR 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 CIKR under their control by:

- Performing comprehensive risk assessments tailored to their specific sector, enterprise, or facility risk landscape;
- Implementing protective actions and programs to reduce identified vulnerabilities appropriate to the level of risk presented;
- Participating in the NIPP sector partnership model (including SCCs and information-sharing mechanisms);
- Developing an awareness of critical dependencies and interdependencies at the sector, enterprise, and facility levels;
- Assisting and supporting Federal, State, local, and tribal government CIKR data collection and protection efforts;
- Developing and coordinating CIKR protective and emergency response actions, plans, and programs with appropriate Federal, State, and local government authorities;
- Establishing continuity plans and programs that facilitate the performance of critical functions during an emergency or until normal operations can be resumed;
- Establishing cybersecurity programs and associated awareness training within the organization;
- Adhering to recognized industry best business practices and standards, including those with a cybersecurity nexus (see appendix 5B);
- Participating in Federal, State, local, and tribal government emergency management programs and coordinating structures;

- Establishing resilient, robust, and/or redundant operational systems or capabilities associated with critical functions;
- Promoting CIKR 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;
- Participating in regular CIKR protection-focused training and exercise programs with other public and private sector partners;
- Identifying and communicating requirements to DHS and/or the SSAs and State and local governments for CIKR protection-related R&D;
- Sharing security-related best practices and entering into operational mutual-aid agreements with other industry partners; and
- Working to identify and reduce barriers to public-private partnerships.

2.2.6 Advisory Councils

Advisory councils provide advice, recommendations, and expertise to the government (e.g., DHS, SSAs, and State or local agencies) regarding CIKR 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 CIKR protection policy and programs, and to make suggestions to increase the efficiency and effectiveness of specific government programs. Examples of CIKR protection-related advisory councils and their associated responsibilities include:

- **Critical Infrastructure Partnership Advisory Council (CIPAC)**: CIPAC is a partnership between government and private sector CIKR owners and operators that facilitates effective coordination of Federal CIKR protection programs. CIPAC engages in a range of CIKR protection activities, such as planning, risk assessments, coordination, NIPP implementation, and operational activities, including incident response and recovery. DHS published a Federal Register Notice on March 24, 2006, announcing the establishment of CIPAC as a Federal Advisory Committee Act (FACA)[5] -exempt body pursuant to section 871 of the Homeland Security Act (see chapter 4).
- **Homeland Security Advisory Council (HSAC)**: 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 governments, public safety, security and first-responder communities, academia, and the private sector.
  - Private Sector Senior Advisory Committee (PVTSAC): The Secretary of Homeland Security established PVTSAC as a subcommittee of HSAC in order to provide HSAC with expert advice from leaders in the private sector.
- **National Infrastructure Advisory Council (NIAC)**: NIAC provides the President, through the Secretary of Homeland Security, with advice on the security of physical and cyber systems across all CIKR sectors. The council comprises up to 30 members appointed by the President. Members are selected from the private sector, academia, and State and local governments. The council was established (and amended) under Executive Orders 13231, 13286, and 13385.
- **National Security Telecommunications Advisory Committee (NSTAC)**: 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. NSTAC, created under Executive Order 12382, comprises up to 30 industry chief executives representing the major communications and network service providers and information technology, finance, and aerospace companies.

2.2.7 Academia and Research Centers

The academic and research center communities play an important role in enabling national-level CIKR protection and implementation of the NIPP, including:

- Establishing Centers of Excellence (i.e., university-based partnerships or federally funded R&D centers) to provide independent analysis of CIKR protection issues;
- Supporting the research, development, testing, evaluation, and deployment of CIKR protection technologies;
- Analyzing, developing, and sharing best practices related to CIKR prioritization and protection efforts;
- Researching and providing innovative thinking and perspective on threats and the behavioral aspects of terrorism;

[5] FACA authorized the establishment of a system governing the creation and operation of advisory committees in the executive branch of the Federal Government and for other purposes. The act, when it applies, generally requires advisory committees to meet in open session and make publicly available associated written materials. It also requires a 15-day notice before any meeting may be closed to public attendance, a requirement that could prevent a meeting on short notice to discuss sensitive information in an appropriate setting.

- Preparing or disseminating guidelines, courses, and descriptions of best practices for physical security and cybersecurity;
- Developing and providing suitable all-hazards risk analysis and risk management courses for CIKR protection professionals;
- Establishing undergraduate and graduate curricula and degree programs;
- Conducting research to identify new technologies and analytical methods that can be applied by partners to support NIPP efforts; and
- Participating in the review and validation of NIPP-supporting risk analysis and management approaches.

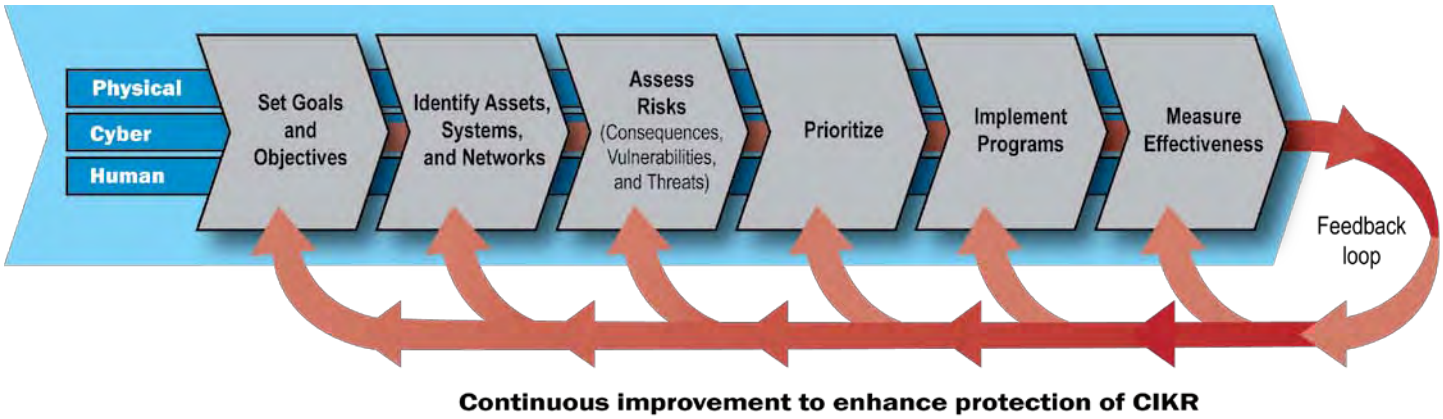
3. The Strategy: Managing Risk

The cornerstone of the NIPP is its risk management framework. Risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. Simply stated, risk is influenced by the nature and magnitude of a threat, the vulnerabilities to that threat, and the consequences that could result. Risk is an important means of prioritizing mitigation efforts for partners ranging from facility owners and operators to Federal agencies. The NIPP risk management framework (see figure 3-1) integrates and coordinates strategies, capabilities, and governance to enable risk-informed decisionmaking related to the Nation's CIKR. This framework is applicable to threats such as natural disasters, manmade safety hazards, and terrorism, although different information and methodologies may be used to understand each.

This chapter addresses the use of the NIPP risk management framework as part of the overall effort to ensure the protection and resiliency of our Nation's CIKR. DHS, the SSAs, and their public and private sector partners share responsibility for implementation of the NIPP risk management framework. The SSAs are responsible for leading sector-specific risk management programs and for ensuring that the tailored, sector-specific application of the risk management framework is addressed in their respective SSPs. DHS supports these efforts by providing guidance and analytical support to the SSAs and other partners. DHS, in collaboration with other CIKR partners, is responsible for using the best available information to conduct cross-sector risk analysis and risk management activities. This includes the assessment of: dependencies, interdependencies, and cascading effects; identification of common vulnerabilities; development and sharing of common threat scenarios; assessment and comparison of risk across sectors; identification and prioritization of risk management opportunities across sectors; development and sharing of cross-sector measures to reduce or manage risk; and identification of specific cross-sector R&D needs.

The NIPP risk management framework is tailored toward and applied on an asset, system, network, or functional basis,

Figure 3-1: NIPP Risk Management Framework



depending on the fundamental characteristics of the individual CIKR sectors. For those sectors primarily dependent on fixed assets and physical facilities, a bottom-up, asset-by-asset approach may be most appropriate. For sectors such as Communications, Information Technology, and Agriculture and Food, with accessible and distributed systems, a top-down, business or mission continuity approach, or risk assessments that focus on network and system interdependencies may be more effective. Each sector must pursue the approach that produces the most effective use of resources for the sector and contributes to cross-sector comparative risk analyses conducted by DHS.

The NIPP risk management framework includes the following activities:

- **Set goals and objectives**: Define specific outcomes, conditions, end points, or performance targets that collectively constitute an effective risk management posture.
- **Identify assets, systems, and networks**: Develop an inventory of the assets, systems, and networks, including those located outside the United States, that make up the Nation's CIKR or contribute to the critical functionality therein, and collect information pertinent to risk management that takes into account the fundamental characteristics of each sector.
- **Assess risks**: Evaluate the risk, taking into consideration the potential direct and indirect consequences of a terrorist attack or other hazards (including, as capabilities mature, seasonal changes in the consequences and dependencies and interdependencies associated with each identified asset, system, or network), known vulnerabilities to various potential attack methods or other significant hazards, and general or specific threat information.
- **Prioritize**: Aggregate and compare risk assessment results to: develop an appropriate view of asset, system, and/or network risks and associated mission continuity, where applicable; establish priorities based on risk; and determine protection, resilience, or business continuity initiatives that provide the greatest return on investment for the mitigation of risk.
- **Implement protective programs and resiliency strategies**: Select appropriate actions or programs to reduce or manage the risk identified; identify and provide the resources needed to address priorities.
- **Measure effectiveness**: Use metrics and other evaluation procedures at the appropriate national, State, local, regional, and sector levels to measure progress and assess the effectiveness of the CIKR protection programs.

This process features a continuous feedback loop, which allows the Federal Government and its CIKR partners to track progress and implement actions to improve national CIKR protection and resiliency over time. The physical, cyber, and human elements of CIKR should be considered in tandem in each aspect of the risk management framework. The sector partnership model discussed in chapter 4 provides the structure for coordination and management of risk management activities that are flexibly tailored to different sectors and levels of government.

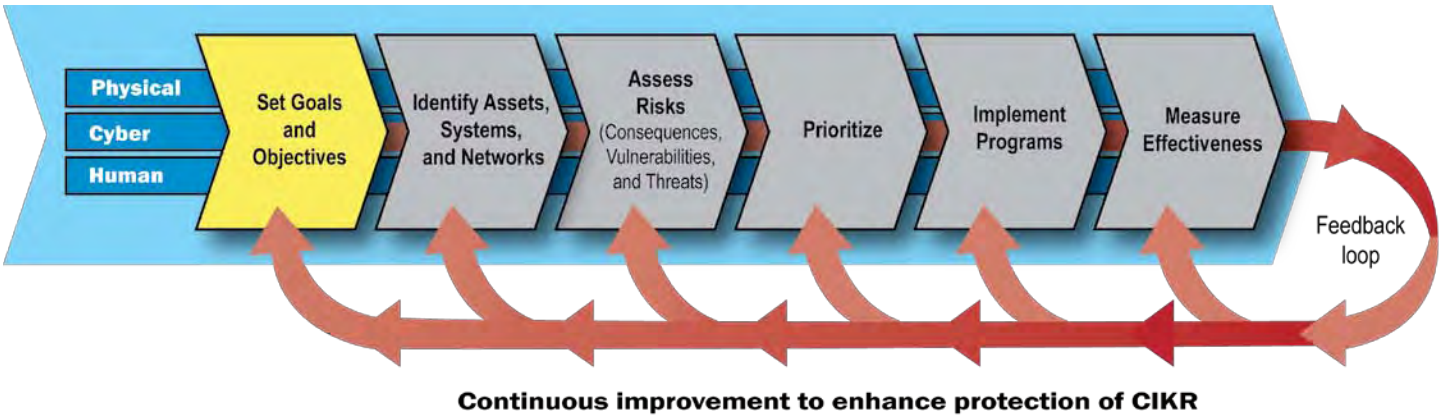
3.1 Set Goals and Objectives

Achieving robust, protected, and resilient infrastructure requires national, State, local, and sector-specific CIKR protection visions, goals, and objectives that describe the desired risk management posture. These goals and objectives should consider the physical, cyber, and human elements of CIKR protection and resiliency. Goals and objectives may vary across and within sectors and levels of government, depending on the risk landscape, operating environment, and composition of a specific industry, resource, or other aspect of CIKR.

Nationally, the overall goal of CIKR-related risk management is an enhanced state of protection and resilience achieved through the implementation of focused risk-reduction strategies within and across sectors and levels of government. The NIPP risk management framework supports this goal by:

- Enabling the development of the national, State, regional, and sector risk profiles that serve as the foundation for the National CIKR Protection Annual Report described in chapter 7. These risk profiles outline the highest risks facing different sectors and geographical regions, and identify cross-sector or regional issues of concern that are appropriate for the Federal CIKR protection focus, as well as opportunities for sector-, State-, and regionally based initiatives.
- Enabling DHS, SSAs, and other partners to determine the best courses of action to reduce potential consequences, threats, or vulnerabilities. Some available options include encouraging voluntary implementation of focused risk management strategies (e.g., through public-private partnerships), pursuing economic incentive-related policies and programs, and undertaking regulatory action, if appropriate; and
- Allowing the identification of risk management and resource allocation options for CIKR owners and operators, as well as different government partners.

Figure 3-2: NIPP Risk Management Framework: Set Goals and Objectives



From a sector or jurisdictional perspective, CIKR protection goals or their related supporting objectives:

- Consider distinct assets, systems, networks, functions, operational processes, business environments, and risk management approaches;
- Define the risk management posture that CIKR partners seek to attain; and
- Express this posture in terms of the outcomes and objectives sought.

Taken collectively, these goals and objectives guide all levels of government and the private sector in tailoring risk management programs and activities to address CIKR protection and resilience needs.

3.2 Identify Assets, Systems, and Networks

To meet its responsibilities under the Homeland Security Act and HSPD-7, DHS continuously engages partner agencies and other CIKR partners to build, manage, refine, and improve a comprehensive inventory of the assets, systems, and networks that make up the Nation's CIKR. This inventory provides a common baseline of knowledge that can support CIKR partners at various levels of government and the private sector in understanding infrastructure dependencies and interdependencies, as well as enable national, local, regional, and sector-based risk assessment, prioritization, and management.

Given the Nation's vast and varied infrastructure, developing an inventory of critical assets, systems, and networks will vary by sector and types of CIKR.

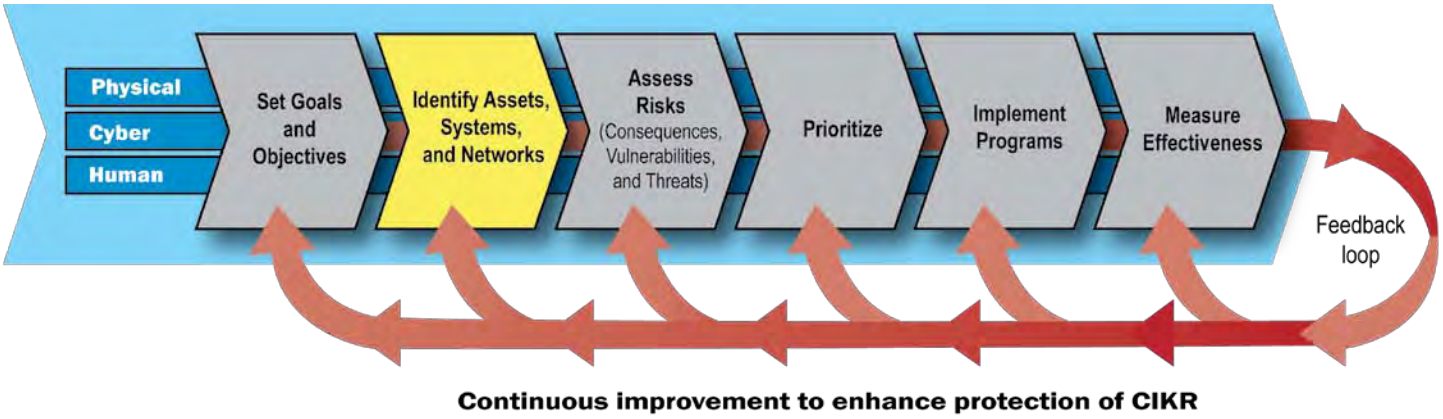
3.2.1 National Infrastructure Inventory

DHS maintains a national inventory of the assets, systems, and networks that make up the Nation's CIKR. The Nation's infrastructure includes assets, systems, and networks that are nationally significant and those that may not be significant on a national level but are, nonetheless, important to State, local, or regional CIKR protection, incident management, and response and recovery efforts. The principal national inventory of CIKR systems and assets is the IDW. The IDW comprises a federated data architecture that provides a single virtual view of one or more infrastructure data sources. DHS uses this data to provide all relevant public and private sector CIKR partners with access to the most current and complete view of the Nation's infrastructure information allowed under applicable Federal, State, or local regulation. Section 3.2.2 discusses protecting and accessing this data.

The goal of the IDW is to provide access to relevant information for natural disasters, industrial accidents, and other incidents, as well as maintain basic information about the relationships, dependencies, and interdependencies among various assets, systems, and networks, including foreign CIKR on which the United States may rely. The inventory will also eventually include a cyber data framework to characterize each sector's unique and significant cyber assets, systems, or networks.

This information is needed not only to help manage CIKR protection and resiliency approaches, but also to inform and support the response to a wide array of incidents and emergencies. Risk may change based on many factors including damage resulting from a natural disaster; seasonal or cyclic dependencies; and changes in technology, the economy, or the terrorist threat. The inventory supports domestic incident

Figure 3-3: NIPP Risk Management Framework: Identify Assets, Systems, and Networks



management by helping to: prioritize and focus preparedness planning; inform decisionmaking; establish strategies for response; and identify priorities for restoration, remediation, and reconstruction.

Currently, the inventory and associated attributes are maintained through the Infrastructure Information Collection System (IICS), a federated IDW, accessible in a geospatial context using the capabilities provided by the Integrated Common Analytical Viewer (iCAV) suite of tools, including the iCAV and DHS Earth viewers. The SSAs and DHS work together and in concert with State, local, tribal, and territorial governments and private sector partners to ensure that the inventory data structure is accurate, current, and secure. DHS provides guidelines concerning information needed to develop and maintain the inventory. Within this inventory, the set of nationally and regionally significant infrastructure is maintained and constantly updated and refined.

Information in the IDW comes from a variety of sources and takes advantage of work that has already been done, such as:

- **Sector inventories**: SSAs and GCCs maintain close working relationships with owners and operators, SCCs, and other sources that maintain the inventories necessary for the sector's business or mission. CIKR partners provide relevant information to DHS and update it on a periodic basis to ensure that sector CIKR and associated critical functionality are adequately represented and that sector and cross-sector dependencies and interdependencies can be identified and analyzed.
- **Voluntary submittals from CIKR partners**: Owners and operators; State, local, tribal, and territorial governments; and Federal departments and agencies voluntarily submit information and previously completed inventories and analyses for DHS to consider.
- **Results of studies**: Various government or commercial databases developed as a result of studies undertaken by trade associations, advocacy groups, and regulatory agencies may contain relevant information.
- **Annual data calls**: DHS, in cooperation with the SSAs and other CIKR partners, conducts a voluntary annual data call to State, territorial, and Federal partners. This data call process allows State, territorial, and Federal partners to propose CIKR data inputs meeting specified criteria.
- **Ongoing reviews of particular locations where risk is believed to be higher**: DHS- and SSA-initiated site assessments to: provide information on vulnerability; help identify assets, systems, and networks and their dependencies, interdependencies, and critical functionality; and provide information that will help quantify their value in risk analyses.

DHS, in coordination with the SSAs, State and local governments, private sector owners and operators, and other partners, works to build from and update existing inventories at the State and local levels to avoid duplication of past or ongoing complementary efforts.

3.2.2 Protecting and Accessing Inventory Information

The Federal Government recognizes the sensitive, business, or proprietary nature of much of the information accessed through the IDW. DHS is responsible for protecting this information from unauthorized disclosure or use. Information in the IDW is protected from unauthorized disclosure or misuse to the maximum extent allowed under applicable Federal, State, or local regulations, including PCII and security classification rules (see section 4.3). Additionally, DHS ensures that all data and licensing restrictions are strictly enforced. DHS is implementing important resilient

and redundant security measures that apply to the IDW and provide system integrity and security, software security, and data protection.

3.2.3 SSA Role in Inventory Development and Maintenance

The SSAs have a leading role in several phases of CIKR inventory development and maintenance, including nominating assets and systems and adjudication of those high-risk assets and systems proposed by States and territories in response to the annual data call.

The specific methods by which the SSAs collect sector-specific asset, system, and network data vary by sector and are described in the individual SSPs. The SSPs include descriptions of mechanisms for making data collection efforts more manageable and less burdensome, such as:

- Prioritizing the approach for data outreach to different partners;
- Identifying assets, systems, networks, or functions of potential national-, regional-, or sector-level importance; and
- Identifying, reviewing, and leveraging existing sector infrastructure data sources.

The SSAs enable sector-specific asset, system, and network awareness, data collection, and information sharing primarily by understanding existing sector-based data sources and by facilitating information-sharing agreements with data owners. For example, DHS, in its capacity as the SSA for the Dams Sector (which includes locks and levees), works closely with the U.S. Army Corps of Engineers (USACE) in the Dams Sector to facilitate data discovery within the National Inventory of Dams (NID). Although owned and maintained by USACE, shared access to the NID provides CIKR partners in Federal, State, and local governments and the private sector with a comprehensive understanding of the national dams landscape.

More details on SSA roles and responsibilities in facilitating sector awareness and understanding related to the IDW are included in appendix 3C.

3.2.4 State and Local Government Role in Inventory Development and Maintenance

State and local government agencies play an important role in understanding the national CIKR landscape by enabling the identification of assets, systems, and networks at the State and local levels. State and local first-responders, emergency managers, public health officials, and others involved in homeland security missions frequently interact with infrastructure owners and operators in their jurisdictions to plan for and respond to all manner of natural and manmade hazards. These relationships form the core of the public-private partnership model and translate into first-hand knowledge of the infrastructure landscape at the State and local levels, as well as an understanding of those CIKR that are considered critical from a State and local perspective.

DHS provides a number of tools and resources to help State and local officials leverage their knowledge to create infrastructure inventories that contribute to the IDW. This includes the Constellation/Automated Critical Asset Management System (C/ACAMS) that helps State and local officials leverage their knowledge to create infrastructure inventories, implement practical CIKR protection programs, and facilitate information sharing within and across State and local boundaries, as well as with DHS and other Federal partners. By sharing first-hand knowledge and understanding through tools such as C/ACAMS, State and local partners contribute directly to the national CIKR protection mission.

Additional information on State roles and responsibilities in this area is contained in appendix 3C.

Constellation/Automated Critical Asset Management System

C/ACAMS is a Web-enabled information services portal that helps State and local governments build CIKR protection programs in their local jurisdictions. Specifically, C/ACAMS provides a set of tools and resources that help law enforcement, public safety, and emergency response personnel to:

- **Collect and use CIKR asset data;**
- **Assess CIKR asset vulnerabilities;**
- **Develop all-hazards incident response and recovery plans; and**
- **Build public-private partnerships.**

The Constellation portion of C/ACAMS is an information gathering and analysis tool that allows users to search a range of free and subscription reporting sources to find relevant information tailored to their jurisdiction's needs. ACAMS is a secure, online database and database management platform that allows for: the collection and management of CIKR asset data; the cataloguing, screening, and sorting of this data; the production of tailored infrastructure reports; and the development of a variety of pre- and post-incident response plans that are useful for strategic and operational planners and tactical commanders. Email ACAMS-info@hq.dhs.gov for additional information.

3.2.5 Identifying Cyber Infrastructure

The NIPP addresses the protection of the cyber elements of CIKR in an integrated manner rather than as a separate consideration. As a component of the sector-specific risk assessment process, cyber infrastructure components should be identified individually or included as a cyber element of a larger asset, system, or network's description if they are associated with one. The identification process should include information on international cyber infrastructure with cross-border implications, interdependencies, or cross-sector ramifications. Cyber infrastructure that exist in most, if not all, sectors include business systems, control systems, access control systems, and warning and alert systems.

The Internet has been identified as a key resource, comprising the domestic and international assets within both the Information Technology and Communications Sectors, and is used by all sectors to varying degrees. While the availability of the service is the responsibility of both the Information Technology and Communications sectors, the need for access to and reliance on the Internet is common to all sectors.

DHS supports the SSAs and other CIKR partners by developing tools and methodologies to assist in identifying cyber assets, systems, and networks, including those that involve multiple sectors. As needed, DHS works with sector representatives to help identify cyber infrastructure within the NIPP risk management framework.

Additionally, DHS, in collaboration with other CIKR partners, provides cross-sector cyber methodologies that, when applied, enable sectors to identify cyber assets, systems, and networks that may have nationally significant consequences if destroyed, incapacitated, or exploited. These methodologies also characterize the reliance of a sector's business and operational functionality on cyber infrastructure components. Also, if an appropriate cyber identification methodology is already being used within the sector, DHS will work with the sector to ensure alignment of that methodology with the NIPP risk management framework.

3.2.6 Identifying Positioning, Navigation, and Timing Services

Space-based and terrestrial positioning, navigation, and timing (PNT) services are a component of multiple CIKR sectors. These services underpin almost every aspect of transportation across all its various modes. Additionally, the Banking and Finance, Communications, Energy, and Water Sectors rely on GPS as their primary timing source. The systems that support or enable critical functions in the CIKR sectors should be identified, either as part of or independent of the infrastructure, as appropriate. Examples of CIKR functions that depend on PNT services include: aviation (navigation, air traffic control, surface guidance); maritime (harbor, inland waterway vessel movement, and maritime surveillance, such as Automatic Identification Systems (AIS)); surface transportation (rail, hazardous materials (HAZMAT) tracking); communications networks (global fiber and wireless networks); and power grids. PNT services must be reliable, seamless, resistant, and resilient to unintentional or intentional interference or jamming.

DHS has developed a PNT Interference Detection and Mitigation (IDM) Plan as required by the U.S. Space-Based PNT Policy of December 8, 2004. The policy established responsibilities for multiple departments and agencies within the Federal Government to better plan, manage, and protect PNT services, and assigned to the DHS specific responsibilities governing the protection of PNT services within CIKR. The IDM Plan details the DHS initial response to the policy implementation action and lays the foundation for further planning and actions necessary to meet the responsibilities. The IDM Plan was approved by the President on August 20, 2007.

3.3 Assess Risks

Common definitions, scenarios, assumptions, metrics, and processes are needed to ensure that risk assessments contribute to a shared understanding among CIKR partners. The approach outlined by the NIPP risk management framework results in sound, scenario-based consequence and vulnerability estimates, as well as an assessment of the likelihood that the postulated threat would occur.

The NIPP framework calls for CIKR partners to assess risk from any scenario as a function of consequence, vulnerability, and threat, as defined below. As stated in the introduction to this chapter, it is important to think of risk as influenced by the nature and magnitude of a threat, the vulnerabilities to that threat, and the consequences that could result:

$$R = f(C,V,T)$$

- **Consequence**: The effect of an event, incident, or occurrence; reflects the level, duration, and nature of the loss resulting from the incident. For the purposes of the NIPP, consequences are divided into four main categories: public health and safety (i.e., loss of life and illness); economic (direct and indirect); psychological; and governance/mission impacts.

- **Vulnerability**: Physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. In calculating the risk of an intentional hazard, a common measure of vulnerability is the likelihood that an attack is successful, given that it is attempted.
- **Threat**: Natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. For the purpose of calculating risk, the threat of an intentional hazard is generally estimated as the likelihood of an attack being attempted by an adversary; for other hazards, threat is generally estimated as the likelihood that a hazard will manifest itself. In the case of terrorist attacks, the threat likelihood is estimated based on the intent and capability of the adversary.

CIKR-related risk assessments consider all three components of risk and are conducted on assets, systems, or networks, depending on the characteristics of the infrastructure being examined. Once the three components of risk have been assessed for one or more given assets, systems, or networks, they must be integrated into a defensible model to produce a risk estimate.

DHS conducts risk analyses for each of the 18 CIKR sectors, working in close collaboration with the SSAs, State and local authorities, and private sector owners and operators. This includes execution of the Strategic Homeland Infrastructure Risk Assessment (SHIRA) data call that provides input to risk analysis programs and projects and considers data collected more broadly through other DHS Office of Infrastructure Protection (IP) program activities as well.

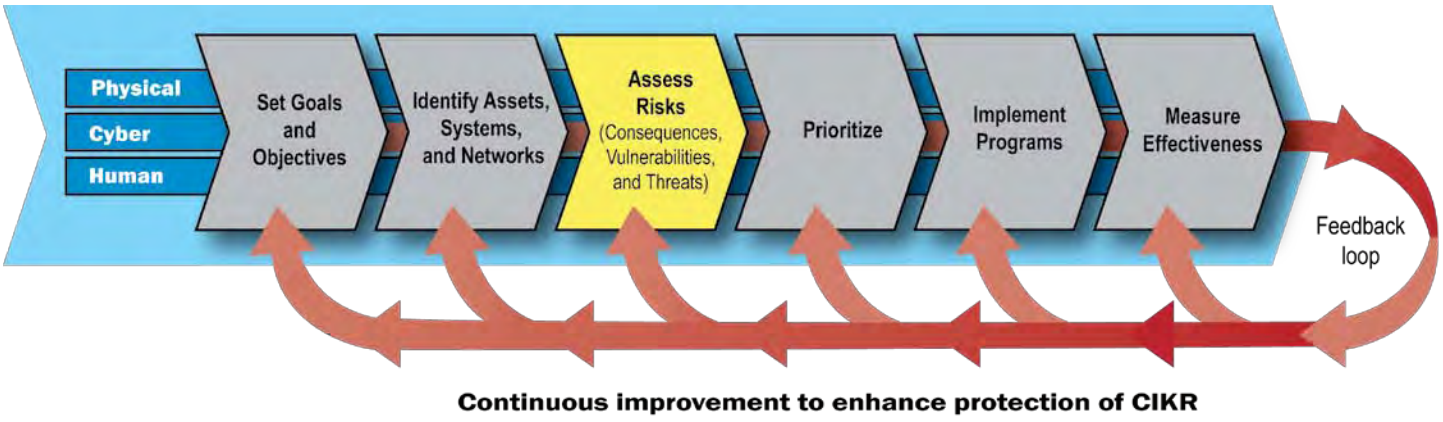
DHS has identified a number of risk assessment characteristics and data requirements to produce results that enable cross-sector risk comparisons; these are termed **core criteria**. These features provide a guide for improving existing methodologies or modifying them so that the investment and expertise they represent can be used to support national-level, comparative risk assessment, investments, incident response planning, and resource prioritization. The NIPP core criteria for risk assessments are summarized in appendix 3A and are discussed below.

A very important program that provides a key synthesizing assessment for the Federal NIPP community is the Strategic Homeland Infrastructure Risk Assessment (SHIRA) process. The SHIRA involves an annual collaborative process conducted in coordination with interested members of the CIKR protection community to assess and analyze the risks to the Nation's infrastructure from terrorism, as well as natural and manmade hazards. The information derived through the SHIRA process feeds a number of analytic products, including the National Risk Profile, the foundation of the National CIKR Protection Annual Report, as well as individual Sector Risk Profiles.

3.3.1 NIPP Core Criteria for Risk Assessments

The NIPP core criteria for risk assessments identify the characteristics and information needed to produce results that can contribute to cross-sector risk comparisons. These criteria include both the analytic principles that are broadly applicable to all parts of a risk methodology and specific guidance regarding information needed to understand and address each of the three components of the risk equation: consequence, vulnerability, and threat. Risk assessments are conducted by many CIKR partners to meet their own decisionmaking needs, using a broad range of methodologies. Whenever possible, DHS seeks to use information from partners' risk assessments to contribute to an understanding of risks across sectors and throughout the Nation. Thus, adherence to the NIPP core criteria will facilitate the broadest applicability of existing assessments.

Figure 3-4: NIPP Risk Management Framework: Assess Risks



Recognizing that many risk assessment methodologies are under development and others evolve in a dynamic environment, the core criteria for risk assessment methodologies also serve as a guide to future adaptations.

The basic analytic principles ensure that risk assessments are:

- **Documented**: The methodology and the assessment must clearly document what information is used and how it is synthesized to generate a risk estimate. Any assumptions, weighting factors, and subjective judgments need to be transparent to the user of the methodology, its audience, and others who are expected to use the results. The types of decisions that the risk assessment is designed to support and the timeframe of the assessment (e.g., current conditions versus future operations) should be given.
- **Reproducible**: The methodology must produce comparable, repeatable results, even though assessments of different CIKR may be performed by different analysts or teams of analysts. It must minimize the number and impact of subjective judgments, leaving policy and value judgments to be applied by decisionmakers.
- **Defensible**: The risk methodology must logically integrate its components, making appropriate use of the professional disciplines relevant to the analysis, as well as be free from significant errors or omissions. Uncertainty associated with consequence estimates and confidence in the vulnerability and threat estimates should be communicated.
- **Complete**: The methodology should assess *consequence*, *vulnerability*, and *threat* for every defined risk scenario and follow the more specific guidance for each of these as given in the subsections that follow. The guidance is also summarized in appendix 3A.

3.3.2 Risk Scenario Identification

All risk is assessed with respect to a specific scenario or set of scenarios. Simply put, the risk scenario answers the question "The risk of what?" All consequence, vulnerability, and threat estimates are specific to the risk scenario. Risks can be assessed for assets, networks, systems, and defined combinations of these. In the case of the risk from terrorism, the subject of the risk assessment is commonly called the target. When developing scenarios for a risk assessment of a relatively fixed system, an important first step is to identify those components or critical nodes where potential consequences would be highest and where protective measures and resiliency strategies can be focused. Open and adaptive systems are likely to require more sophisticated approaches to screening, which are still under development.

The risk scenario also identifies the potential source of harm. For terrorism, the risk scenario must include the means of attack and delivery, such as a 4000-pound TNT-equivalent, vehicle-borne improvised explosive device (VBIED). In the case of natural hazards, the risk scenario must include the type and magnitude of the hazard (e.g., a Category 5 hurricane or an earthquake of 6.5 on the Richter scale).

Finally, the scenario must identify the conditions that are relevant to calculating consequence, vulnerability, and threat. DHS uses reasonable worst-case conditions to assess terrorism risks because intelligent adversaries can choose circumstances where targets are vulnerable and consequences are maximized. The concept of "worst case" (that combination of conditions that would make the most harmful results the ones that occur) is moderated by reason. Scenarios should not be compounded in complexity to include numerous unlikely conditions, unless the focus of the contingency and other planning is on extremely rare events. Neither should scenarios be based simply on average conditions. Each type of target will have the different characteristics needed to accurately describe reasonable worst-case conditions, such as a stadium's maximum capacity, the storage volume of a particularly hazardous material at a chemical facility, or the height and duration of a high water level at a dam.

3.3.3 Consequence Assessment

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

- **Public Health and Safety**: Effect on human life and physical well-being (e.g., fatalities, injuries/illness).[6]
- **Economic**: Direct and indirect economic losses (e.g., cost to rebuild asset, cost to respond to and recover from attack, downstream costs resulting from disruption of product or service, long-term costs due to environmental damage).
- **Psychological**: Effect on public morale and confidence in national economic and political institutions. This encompasses those changes in perceptions emerging after a significant incident that affect the public's sense of safety and well-being and can manifest in aberrant behavior.

[6] Injuries and illnesses are not commonly assessed at this point; however, the capability exists to develop this information and NIPP partners should move toward including it when it is relevant and possible.

- **Governance/Mission Impact**: Effect on government's or industry's ability to maintain order, deliver minimum essential public services, ensure public health and safety, and carry out national security-related missions.

Under the general rubric of governance/mission impact are several discrete, federally mandated missions that may be disrupted. Although many of these missions are directly fulfilled by government agencies, some are fulfilled or supported by the private sector; however, government actions can serve to either foster a healthy environment for them or inadvertently disrupt them. These include the responsibility to: ensure national security and perform other Federal missions; ensure public health; maintain order; enable the provision of essential public services; and ensure an orderly economy.

There are indirect and cascading impacts of disruptions that are difficult to understand and may be even more difficult to appraise. Some may already be accounted for in estimates of economic losses, while others may require further metrics development to enable them to be considered in a more comprehensive risk assessment. Ongoing work with NIPP partners will pursue solutions to these challenges, aiming to improve our ability to compare and prioritize mission-disruption losses in addition to the other types of consequences of concern.

A full-consequence assessment takes into consideration all four consequence criteria; however, estimating potential indirect impacts requires the use of numerous assumptions and other complex variables. An assessment of all categories of consequence may be beyond the capabilities available (or the precision needed) for a given risk assessment. At a minimum, assessments should focus on the two most fundamental impacts—the human consequences and the most relevant direct economic consequences.

3.3.3.1 Consequence Assessment Methodologies That Enable National Risk Analysis

DHS works with CIKR partners to develop or improve consequence assessment methodologies that can be applied to a variety of asset, system, or network types and to produce comparable quantitative consequence estimates. Many tools and methods can support the assessment of direct effects and consequences and are often sector-specific. Consequence analysis should ideally address both direct and indirect effects. Many assets, systems, and networks depend on connections to other CIKR to function. For example, nearly all Sectors share relationships with elements of the Energy, Information Technology, Communications, Banking and Finance, and Transportation Systems sectors. In many cases, the failure of an asset or system in one sector will affect the ability of interrelated assets or systems in the same or another sector to perform the necessary functions. Furthermore, cyber interdependencies present unique challenges for all sectors because of the borderless nature of cyberspace. Interdependencies are dual in nature (e.g., the Energy Sector relies on computer-based control systems to manage the electric power grid, while those same control systems require electric power to operate). As a result, complete consequence analysis addresses both CIKR interconnections for the purposes of NIPP risk assessment.

Various Federal and State entities, including national laboratories, are developing sophisticated models and simulations to identify dependencies and interdependencies within and across sectors. The Federal Government established the National Infrastructure Simulation and Analysis Center (NISAC) to support these efforts (see section 6.4.2). NISAC is chartered to develop advanced modeling, simulation, and analysis capabilities for the Nation's CIKR. These tools and analyses address dependencies and interdependencies, both physical and cyber, in an all-hazards context. These sophisticated models enhance the Nation's understanding of CIKR dependencies and interdependencies to better inform decisionmakers, especially for cross-sector priorities.

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

3.3.3.2 Consequence Uncertainty

There is an element of uncertainty in consequence estimates. Even when a scenario with reasonable worst-case conditions is clearly stated and consistently applied, there is often a range of outcomes that could occur. For some incidents, the consequence range is small and a single estimate may provide sufficient information to support decisions. If the range of outcomes is large, the scenario may require more specificity about conditions to obtain appropriate estimates of the outcomes. However, if the scenario is broken down to a reasonable level of granularity and there is still significant uncertainty, the single estimate should be accompanied by the uncertainty range to support more informed decisionmaking. The best way to communicate uncertainty will depend on the factors that make the outcome uncertain, as well as the amount and type of information that is available.

Core Criteria Guidance for Consequence Assessments

- Document the scenarios assessed, tools used, and any key assumptions made.
- Estimate the number of fatalities, injuries, and illnesses, where applicable and feasible, keeping each separate estimate visible to the user.
- Estimate the economic loss in dollars, stating which costs are included (e.g., property damage losses, lost revenue, loss to the economy) and what duration was considered.
- If monetizing human health consequences, document the value(s) used and the assumptions made.
- Consider and document any protective or consequence mitigation measures that have their effect after the incident has occurred, such as the rerouting of systems or HAZMAT or fire-and-rescue response.
- Describe psychological impacts and mission disruption where feasible.

3.3.4 Vulnerability Assessment

Vulnerabilities are physical features or operational attributes that render an entity open to exploitation or susceptible to a given hazard. Vulnerabilities may be associated with physical (e.g., a broken fence), cyber (e.g., lack of a firewall), or human (e.g., untrained guards) factors.

A vulnerability assessment can be a stand-alone process or part of a full risk assessment. The vulnerability assessment involves the evaluation of specific threats to the asset, system, or network under review to identify areas of weakness that could result in consequences of concern.

3.3.4.1 Vulnerability Assessment Methodologies That Enable National Risk Analysis

Many different vulnerability assessment approaches are used in the different CIKR sectors and by various government authorities. The primary vulnerability assessment methodologies used in each sector are described in the respective SSPs. The SSPs also provide specific details regarding how the assessments can be carried out (e.g., by whom and how often). The results of the vulnerability assessments need to be comparable in order to contribute to national-level, cross-sector risk analysis. As with risk assessments, vulnerability assessments should meet the same core criteria (i.e., be documented, objective, defensible, and complete) if the results are to be compared at a national, cross-sector level. In addition, vulnerability-specific core criteria guidance is provided at the end of this section.

3.3.4.2 SSA and DHS Analysis Responsibilities

SSAs and their sector partners are responsible for collecting and documenting the vulnerability assessment approaches used within their sectors. Owners or operators typically perform the vulnerability assessments, sometimes with facilitation by government authorities. The SSAs are also responsible for compiling, where possible, vulnerability assessment results for use in sector and national risk analysis efforts. In addition, the SSAs work with DHS, where possible, to review the results of assessments for assets, systems, and networks that are of greatest concern from the SSA's perspective. The SSAs should strive to involve owners and operators in this effort. Vulnerability assessment information may be submitted by owner/operators for validation as PCII under the PCII Program (see section 4.3, Protection of Sensitive CIKR Information). The PCII Program Manager may designate some information as "categorically included" PCII (see section 4.3.1, Protected Critical Infrastructure Information Program). This designation provides the SSA with the option to receive the categorically included Critical Infrastructure Information (CII) directly from the submitter. This arrangement is based on pre-approval from the PCII Program Office on a case-by-case basis.

DHS works to ensure that appropriate vulnerability assessments are performed for nationally critical CIKR. DHS works with CIKR owners and operators, the SSAs, and appropriate State and local authorities, to either perform the assessment or to verify the adequacy and relevance of previously performed assessments to support risk management decisions.

California Water System Comprehensive Review

Federal, State, and local stakeholders collaborated successfully to complete the first systems-based Comprehensive Review (CR). A systems-based CR is a cooperative government-led analysis of CIKR facilities. The California Water System CR required extensive coordination, planning, research, data collection, and outreach to State and local partners to identify critical assets and system interdependencies. DHS, in conjunction with Federal and California State partners, worked with facility owners and operators to identify critical water system assets. This system consists of 161 assets spanning 33 counties. The review determined that 40 of the 161 assets were critical assets. DHS completed 32 onsite vulnerability assessments and six Emergency Services Capabilities Assessments. DHS met with site owners and operators, California State and local law enforcement, and emergency management entities to analyze and track the gaps, potential enhancements, and protective measures that were identified and to evaluate vulnerability mitigation and grant funding effectiveness.

DHS and the SSAs collaborate to support vulnerability assessments that address the specific needs of the NIPP's approach to CIKR protection and risk management. Such assessments may:

- More fully investigate dependencies and interdependencies;
- Serve as a basis for developing common vulnerability reports that can help identify strategic needs for protective programs or R&D across sectors or subsectors;
- Fill gaps when sectors or owner/operators have not yet completed assessments and decisionmaking requires such studies immediately; and
- Test and validate new methodologies or streamlined approaches for assessing vulnerability.

In some sectors and subsectors, 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 assist in closing this gap, DHS works with the SSAs, owners and operators, and other CIKR partners to provide the following:

- Vulnerability assessment tools that may 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;
- Recommendations regarding the frequency of assessments, particularly in light of emergent threats;

DHS National Cybersecurity Division (NCSD) has developed the Cyber Security Vulnerability Assessment (CSVA), a flexible and scalable approach that analyzes an entity's cybersecurity posture and describes gaps and targeted considerations that can reduce overall cyber risks. It assesses the policies, plans, and procedures in place to reduce cyber vulnerability in 10 categories (e.g., access control, configuration management, physical security of cyber assets, etc.) and leverages various recognized standards, guidance, and methodologies (e.g., the International Organization for Standardization 27001, the Information Systems Audit and Control Association (ISACA) Control Objects for Information and Related Technology (COBIT), and the National Institute of Standards and Technology Special Publication 800 series).

Core Criteria Guidance for Vulnerability Assessments

- **Identify the vulnerabilities associated with physical, cyber, or human factors (openness to both insider and outsider threats), critical dependencies, and physical proximity to hazards.**
- **Describe all protective measures in place and how they reduce the vulnerability for each scenario.**
- **In evaluating security vulnerabilities, develop estimates of the likelihood of an adversary's success for each attack scenario.**
- **For natural hazards, estimate the likelihood of the incident causing harm to the asset, system, or network, given that the natural hazard event occurs at the location of interest for the risk scenario.**

- Site assistance visits and vulnerability assessments of specific CIKR as requested by owners and operators, when resources allow; and
- Cyber vulnerability assessment best practices. (DHS works to leverage established methodologies that have traditionally focused on physical vulnerabilities by enhancing them to better address cyber elements.)

Some vulnerability assessments will include both vulnerability analysis and consequence analysis for specified scenarios.

3.3.5 Threat Assessment

The remaining factor to be considered in the NIPP risk assessment process is the assessment of threat. 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 provides its partners with Federal Government-coordinated unclassified assessments of potential terrorist threats and appropriate access to classified assessments where necessary and authorized. These threat assessments are derived from analyses of adversary intent and capability, and describe what is known about terrorist interest in particular CIKR sectors, as well as specific attack methods. Since international terrorists, in particular, have continually demonstrated flexibility and unpredictability, DHS and its partners in the Intelligence Community also analyze known terrorist goals, objectives, and developing capabilities to provide CIKR owners and operators with a broad view of the potential threat and postulated terrorist attack methods.

TRIPwire Community Gateway

The *TRIPwire* Community Gateway (TWCG) is a new *TRIPwire* Web portal designed specifically for the Nation's CIKR owners, operators, and private security personnel. TWCG provides expert threat analyses, reports, and relevant planning documents to help key private sector partners anticipate, identify, and prevent improvised explosive device (IED) incidents. TWCG shares IED-related information tailored to each of the 18 sectors of CIKR. Sector partners benefit from increased communication, improved awareness of emerging threats, and access to resources and guidance on specific IED preventive and protective measures for their facilities and requirements.

3.3.5.1 Key Aspects of the Terrorist Threat to CIKR

Analysis of terrorist goals and motivations reveals that domestic and international CIKR are potentially prime targets for terrorist attack. Given the deeply rooted nature of these goals and motivations, CIKR likely will remain highly attractive targets for terrorists. Threat assessments must address the various elements of CIKR—physical, cyber, and human—depending on the attack type and target. Physical attacks, including the exploitation of physical elements of CIKR, represent the attack method most frequently used overtly by terrorists. In addition, there is increasing indication of terrorists' intent to conduct cyber attacks and exploit the knowledge, influence, and access of insiders.

3.3.6 Homeland Infrastructure Threat and Risk Analysis Center

The DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) conducts integrated threat and risk analyses for CIKR sectors. HITRAC is a joint intelligence center that spans both the DHS Office of Intelligence and Analysis (I&A)—a member of the Intelligence Community—and IP. As called for in section 201 of the Homeland Security Act, HITRAC brings together intelligence and infrastructure specialists to ensure a sufficient understanding of the risks to the Nation's CIKR from foreign and domestic threats. HITRAC works in partnership with the U.S. Intelligence Community and national law enforcement to integrate and analyze intelligence and law enforcement information in threat and risk analyses products. HITRAC also works in partnership with the SSAs and owners and operators to ensure that their expertise on infrastructure operations is integrated into HITRAC analyses.

HITRAC develops analytical products by combining threat assessments based on all-source information and intelligence analysis with vulnerability and consequence assessments. This process provides an understanding of the threats, CIKR vulnerabilities, and potential consequences of attacks and other hazards. Analyses may also include potential options for managing risk. This combination of intelligence and practical CIKR knowledge allows DHS to provide products that contain strategically relevant and actionable information. It also allows DHS to identify intelligence collection requirements in conjunction with CIKR partners so that the Intelligence Community can provide the type of information necessary to support the CIKR risk management and protection missions. HITRAC coordinates closely with partners outside the Federal Government through the SSAs, SCCs, GCCs, Information Sharing and Analysis Centers (ISACs), State and Local Fusion Centers, and State Homeland Security Offices to ensure that its products are relevant to partner needs and are accessible.

3.3.6.1 Threat and Incident Information

DHS leverages, on a 24/7 basis, intelligence and operations monitoring and reporting from multiple sources to provide analyses based on the most current information available on threats, incidents, and infrastructure status. The timely analysis of information provided by DHS is of unique value to CIKR partners and helps them determine if changes are needed in steady-state and threat-based CIKR risk management measures.

Core Criteria Guidance for Threat Assessments

For adversary-specific threat assessments:

- Account for the adversary's ability to recognize the target and the deterrence value of existing security measures.
- Identify any attack methods that may be employed.
- Consider the level of capability that an adversary demonstrates for a particular attack method.
- Consider the degree of the adversary's intent to attack the target.
- Estimate threat as the likelihood that the adversary would attempt a given attack method against the target.
- If threat likelihoods cannot be estimated, use conditional risk values (consequence times vulnerability) and conduct sensitivity analyses to determine how likely the scenario would have to be to support the decision.

For natural disasters and accidental hazards:

- Use best-available analytic tools and historical data to estimate the likelihood of these events affecting CIKR.

DHS uses a variety of tools and systems to support incident and threat warnings. iCAV and DHS Earth help visualize these incident reports and threat warnings, allowing analysts to deliver a geospatial context to numerous information systems. It facilitates fusing information from multiple suspicious activity sources and provides situational awareness tracking for disasters such as hurricanes and other real-time events. This fusion provides DHS, States, local jurisdictions, and the private sector with a rapid, common understanding of the relationships between these events to support coordinated risk-mitigation, preparedness, response, and recovery activities.

DHS also supports SLFC efforts by ensuring that relevant threat information is passed along in a timely manner to SLFCs, that analyses conducted by national intelligence centers such as HITRAC are readily available to SLFC partners, and that initiatives designed to share best practices related to CIKR identification, risk analysis, and prioritization are supported.

Specialized products that directly support the NIPP and the SSPs include incident reports and threat warnings, which are made available to appropriate partners.

Incident Reports: DHS monitors information on incidents to provide reports that CIKR owners and operators and other decisionmakers can use when considering how evolving incidents might affect their CIKR protection posture. This reporting provides a responsive and credible source to verify or expand on information that CIKR partners may receive initially through the news media, the Internet, or other sources. DHS works with multiple government and private sector operations and watch centers to combine situation reports from law enforcement, intelligence, and private sector sources with infrastructure status and operational expertise to rapidly produce reports from a trusted source. These help inform the decisions of owners and operators regarding changes in risk-mitigation measures that are needed to respond to incidents in progress, such as rail or subway bombings overseas that may call for precautionary actions domestically.

Strategic Threat Assessments: HITRAC works with the Intelligence Community and with DHS's partners to analyze information on adversaries who pose a threat to CIKR. HITRAC provides a high-level assessment of terrorist groups and other adversaries to the SSAs in order to inform their SSPs and prioritization efforts.

Threat Warnings: DHS monitors the flow of intelligence, law enforcement, and private sector security information on a 24/7 basis in light of the business, operational, and status expertise provided by its infrastructure analysis and owner/operator partners to produce relevant threat warnings for CIKR protection. The fusion of intelligence and infrastructure analysis clarifies the implications of intelligence reporting about targeted locations or sectors, potential attack methods and timing, or the specific nature of an emerging threat.

3.3.6.2 Risk Analysis

HITRAC uses risk analysis and other approaches to aid CIKR partners in identifying, assessing, and prioritizing risk management approaches. HITRAC also develops specialized products for strategic planning that directly support the NIPP and SSPs. In addition to these specific products, HITRAC produces strategic assessments and trend analyses that help define the evolving risk to the Nation's CIKR.

- **National Infrastructure Risk Analysis Program**: National, State, regional, cross-sector, sector-specific, and site-specific risk analyses and assessments aid decisionmakers with planning and prioritizing risk-reduction measures within and across the CIKR sectors. These analyses and assessments leverage a number of analytic approaches, including the SHIRA process, which are tailored to particular decisions.
- **National CIKR Prioritization Program**: HITRAC works with CIKR partners to identify and prioritize the assets, systems, and networks most critical to the Nation through the Tier 1 and Tier 2 Program for critical assets, systems, networks, nodes, and functions within the United States, and the Critical Foreign Dependencies Initiative (CFDI) for CIKR outside of the United States. The prioritization of CIKR guides the Nation's protective and incident management responses.
- **Infrastructure Risk Analysis Partnership Program (IRAPP)**: IRAPP assists partners interested in pursuing their own CIKR risk analysis, whether they are in the Federal, State, local, or private sector CIKR protection communities. IRAPP involves customized support to interested partners and the sharing of best practices across the CIKR protection community.
- **Committee on Foreign Investment in the United States (CFIUS) Support**: CFIUS is an interagency committee of the Federal Government that reviews the national security implications of foreign investments of U.S. companies or operations. HITRAC provides support to CFIUS by developing written threat and risk assessments of foreign direct investment in the United States and evaluating the potential risks posed by foreign acquisition of U.S. CIKR. HITRAC also supports DHS efforts to manage those risks through the interagency CFIUS process.
- **Critical Infrastructure Red Team (CIRT)**: The CIRT program focuses its analysis on high-risk sectors/subsectors and high-risk attack methods from the perspective of our Nation's adversaries by conducting open-source analysis,

developing operational plans, and exercising these scenarios through tabletop exercises and developing lessons learned from those activities. These efforts identify gaps in current strategies and risk-reduction programs for the Nation's CIKR and support the development of recommendations for closing or managing identified gaps.

- **Risk Analysis Development Program**: The Risk Analysis Development Program works to improve the capabilities available to CIKR risk analysts and risk managers, both in DHS and among the rest of the NIPP stakeholders. The program conducts R&D to identify sound, common risk analysis approaches that support cross-sector comparisons and the full range of risk management decisions. Such practices use the risk assessment core criteria summarized in appendix 3A as a foundation, but also require the use of common scenarios and assumptions. These capabilities are being tested and are evolving to overcome lingering challenges as risk analysis practices for homeland security mature.
- **Critical Foreign Dependencies Initiative (CFDI)**: CFDI, as part of the larger National CIKR Prioritization Program, is the Nation's first step toward the identification and prioritization of the Nation's critical foreign dependencies. The program provides a consolidating and coordinating mechanism by which the Federal Government may more effectively and efficiently engage our foreign CIKR partners.

3.4 Prioritize

Prioritizing risk management efforts regarding the most significant CIKR helps focus planning, increase coordination, and support effective resource allocation and incident management, response, and restoration decisions.

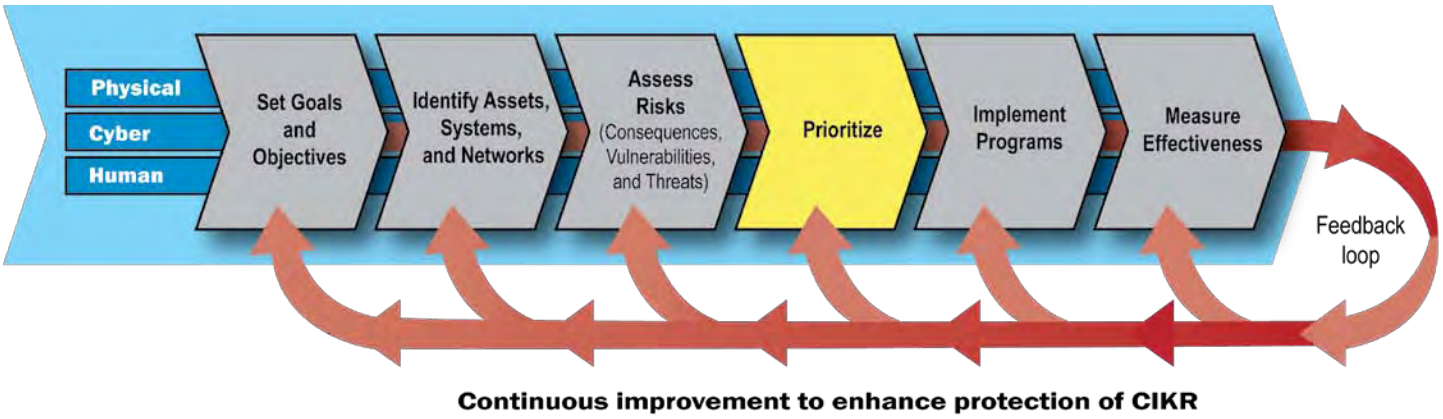
The NIPP risk management framework is applicable to risk assessments on an asset, system, network, function, national, State, regional, or sector basis. Comparing the risk faced by different entities helps identify where risk mitigation is needed and to subsequently determine and help justify the most cost-effective risk management options. This approach identifies which CIKR should be given priority for risk reduction and which alternative options represent the best investment based on their risk-reduction return on investment. The prioritization process also develops information that can be used during incident response to help inform decisionmakers regarding issues associated with CIKR restoration.

3.4.1 The Prioritization Process

The prioritization process involves aggregating, combining, and analyzing risk assessment results to determine which assets, systems, networks, sectors, or combinations of these face the highest risk so that risk management priorities can be established. It also provides the basis for understanding potential risk-mitigation benefits that are used to inform planning and resource decisions.

This process involves two related activities: The first determines which regions, sectors, or other aggregation of CIKR assets, systems, or networks have the highest risk from relevant incidents or events. Of those with similar risk levels, the CIKR with the highest expected losses are accorded the highest priority in risk management program development. The second activity determines which actions are expected to provide the greatest mitigation of risk for any given investment. The risk management initiatives that result in the greatest risk mitigation for the investment proposed are accorded the highest priority in program design, resource allocation, budgeting, and implementation. Other priorities may be set based on regulatory or statutory requirements, presidential directives, and congressional mandates. This approach ensures that programs make the greatest contribution possible to overall CIKR risk mitigation given the

Figure 3-5: NIPP Risk Management Framework: Prioritize



National CIKR Prioritization Program

The DHS Tier 1 and Tier 2 Program identifies nationally significant critical assets and systems in order to enhance decision-making related to CIKR protection. CIKR identified through the program include those that, if destroyed or disrupted, could cause some combination of significant casualties, major economic losses, or widespread and long-term disruptions to national well-being and governance capacity.

The overwhelming majority of the assets and systems identified through this effort are classified as Tier 2. Only a small subset of assets meet the Tier 1 consequence threshold—those whose loss or damage could result in major national or regional impacts similar to the impacts of Hurricane Katrina or the September 11, 2001, attacks. The process of identifying these nationally significant assets and systems is conducted on an annual basis and relies heavily on the insights and knowledge of a wide array of public and private sector security partners.

CIKR categorized as Tier 1 or Tier 2 as a result of this annual process provide a common basis on which DHS and its security partners can implement important CIKR protection programs and initiatives, such as various grant programs, buffer zone protection efforts, facility assessments and training, and other activities. Specifically, the Tier 1/Tier 2 list is used to support eligibility determinations for Urban Area Security Initiative (UASI), State Homeland Security, and Buffer Zone Protection grant programs. The Tier 1/Tier 2 list is classified.

To meet the growing need for additional prioritized lists of infrastructure for planning and incident management purposes, the National CIKR Prioritization Program has also expanded to: identify, assess, and prioritize foreign infrastructure critical to the Nation through CFDI; provide sectors and States with the opportunity to build lists to meet their individual risk and incident management needs; and provide a forum through which the infrastructure protection community can and will continue to improve its ability to prioritize CIKR during incidents and enable response and recovery operations.

available resources. In light of emerging threats, the need to address current credible threat information may require shifting resources.

Assessments become more complex and difficult at different aggregations, such as when comparisons are necessary across sectors, across different geographic areas, or against different types of events. Using a common approach with consistent assumptions and metrics increases the ability to make such comparisons. Without this consistency, assessments are much more challenging.

3.4.2 Tailoring Prioritization Approaches to Sector and Decisionmakers' Needs

CIKR partners rely on different approaches to prioritize risk management activities according to their authorities, specific sector needs, risk landscapes, security approaches, and business environment. For example, owners and operators, Federal agencies, and State and local authorities all have different options available to them to help reduce risk. Asset-focused priorities may be appropriate for CIKR whose risk is predominantly associated with facilities, the local environment, and physical attacks, especially those that can be exploited and used as weapons. Function-focused priorities may more effectively ensure the continuity of operations in the event of a terrorist attack or natural disaster in sectors where CIKR resilience may be more important than CIKR hardening. Programs to reduce CIKR risk give priority to investments that protect physical assets or ensure resilience in virtual systems, depending on which option best enables cost-effective CIKR risk management.

To ensure a consistent approach to risk analysis for CIKR protection, partners establish priorities using risk analyses that use common scenarios and assumptions and follow the parameters for risk assessment methodologies set out in appendix 3A. For quick-response decisions, lacking

Critical Foreign Dependencies Initiative

CFDI involves three phases of activities, two on an annual basis and one ongoing:

- Phase I—Identification (annual): DHS, working with CIKR protection and intelligence community partners, developed the first-ever National Critical Foreign Dependencies List in FY2008, reflecting the critical foreign dependencies of the CIKR sectors, as well as critical foreign dependencies of interest to the Nation as a whole. The identification process includes input from public and private sector CIKR partners.
- Phase II—Prioritization (annual): DHS, working with CIKR partners, and in particular DOS, prioritized the National Critical Foreign Dependencies List based on factors such as the overall criticality of the CIKR to the United States and foreign partner willingness and capability to engage in collaborative risk management activities.
- Phase III—Engagement (ongoing): Phase III involves leveraging the prioritized National Critical Foreign Dependencies List to guide current and future U.S. bilateral and multilateral incident and risk management activities with foreign partners. DHS and DOS established mechanisms to ensure coordinated engagement and collaboration by public sector entities, in partnership with the private sector.

sound risk assessments for reference, some priorities will be informed by top-down assessments using surrogate data or data at high levels of CIKR aggregation (e.g., population density as a surrogate for casualties). As both the NIPP partnership and the knowledge base of risk assessments grow, decisions can be increasingly informed by a combination of top-down and bottom-up analyses using detailed information on specific individual facilities, with a prioritization based on the level of risk reduced by the investment.

3.4.3 The Uses of Prioritization

A primary use of prioritization is to inform resource allocation decisions, such as: where risk management programs should be instituted; guidance on investments in these programs; and which measures offer the greatest return on investment. The results of the prioritization process guide CIKR risk management requirements and should drive important resource allocation decisions.

At the national level, DHS is responsible for overall national risk-informed CIKR prioritization in close collaboration with the SSAs, States, and other CIKR partners. SSA responsibilities include managing government interaction with the sector and helping to cultivate information sharing and collaboration to identify, prioritize, and manage risk. They must also extend their sector focus to enable cross-sector comparisons of risk and metrics that help owners and operators, as well as Federal, State, local, and tribal governments, support evaluations of the risk-reduction return on various investments. At the State level, DHS is working to develop a collaborative relationship with State and local authorities through the Infrastructure Risk Analysis Partnership Program. This effort is geared toward working with State authorities to foster the capability to develop, evaluate, and support the implementation of CIKR risk management decisions in a State/local environment. The program is initially being piloted with a limited group of CIKR partners and will subsequently be rolled out more broadly as the roles, responsibilities, and approaches are tested and refined.

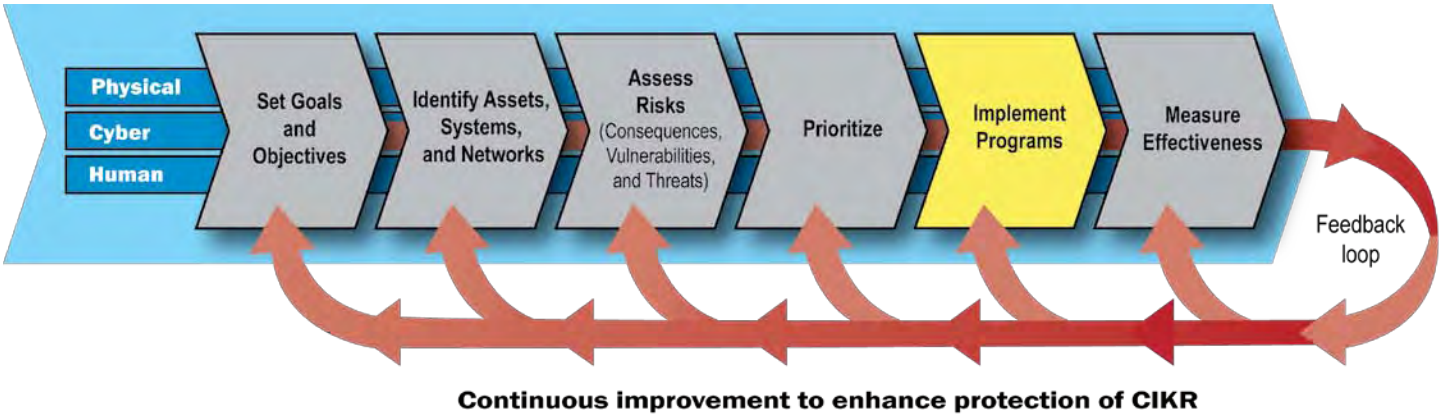
The National CIKR Risk Profile

Leveraging information provided through the SHIRA process, HITRAC produces a National CIKR Risk Profile that serves as the foundation of the infrastructure protection community's common prioritization of risks to the Nation's infrastructure and is captured in the National CIKR Protection Annual Report. Each year, the National Risk Profile identifies the highest relative risks to CIKR from among a number of natural and manmade hazards, as well as those sectors at a higher risk from the greatest number of hazards. The report also identifies additional risk management concerns, such as high-likelihood risks and low-likelihood/high-consequence infrastructure protection priorities. By providing a common understanding of the Nation's CIKR risks, the National Risk Profile provides a common basis for prioritization and helps to focus community efforts on those hazards and sectors of greatest overall concern.

3.5 Implement Protective Programs and Resiliency Strategies

The risk assessment and prioritization process at the sector and jurisdictional levels will help identify requirements for near-term and future protective programs and resiliency strategies. Some of the identified shortfalls or opportunities for improvement will be filled by owner/operators, either voluntarily or based on various incentives. Other shortfalls will be addressed

Figure 3-6: NIPP Risk Management Framework: Implement Programs



through the protective programs that each sector develops under the SSP, in State CIKR protection plans, or through cross-sector or national initiatives undertaken by DHS.

The Nation's CIKR is widely distributed in both a physical and logical sense. Effective CIKR protection requires both distributed implementation of protective programs by partners and focused national leadership to ensure implementation of a comprehensive, coordinated, and cost-effective approach that helps reduce or manage the risks to the Nation's most critical assets, systems, and networks. At the implementation level, protective programs and resiliency strategies consist of numerous, diverse actions that are undertaken by various CIKR partners. From the leadership perspective, programs are structured to address coordination and cost-effectiveness.

The following sections describe the nature and characteristics of best practice protective programs and resiliency strategies, as well as some existing programs that could be applied to specific assets, systems, and networks.

3.5.1 Risk Management Actions

Risk management actions involve measures designed to: prevent, deter, and mitigate the threat; reduce vulnerability to an attack or other disaster; minimize consequences; and enable timely, efficient response and restoration in a post-event situation, whether a terrorist attack, natural disaster, or other incident. The NIPP risk management framework focuses attention on those activities that bring the greatest return on investment, not simply the vulnerability reduction to be achieved. Protective programs and resiliency strategies vary between sectors and across a wide spectrum of activities designed to deter, devalue, detect, or defend.

Risk management actions also may include the means for mitigating the consequences of an attack or incident. These actions are focused on mitigation, response, and/or recovery. Generally, it is considered more cost-effective to build security and resiliency into assets, systems, and networks than to retrofit them after initial development and deployment. Accordingly, CIKR partners should consider how risk management, robustness, resiliency, and appropriate physical security and cybersecurity enhancements could be incorporated into the design and construction of new CIKR.

In situations where robustness and resiliency are keys to CIKR protection, providing protection at the system level rather than at the individual 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 and Resiliency Strategies

Characteristics of effective CIKR protective programs and resiliency strategies include, but are not limited to, the following:

- **Comprehensive**: Effective programs must address the physical, cyber, and human elements of CIKR, as appropriate, and consider long-term, short-term, and sustainable activities. The SSPs describe many programs and initiatives to protect CIKR within the sector (e.g., operational changes, physical protection, equipment hardening, cyber protection, system resiliency, backup communications, training, response plans, and security system upgrades).
- **Coordinated**: Because of the highly distributed and complex nature of the various CIKR sectors, the responsibility for protecting CIKR must be coordinated:
  - CIKR owners and operators (public or private sector) are responsible for protecting property, information, and people through measures that manage 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, keeping computer software and virus-checking applications up to date, and applying fixes for known software defects).
  - 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 relevant Federal programs such as the Buffer Zone Protection Program (BZPP), and provide specific law enforcement capabilities as needed. When appropriate, they have access to Federal resources to meet jurisdictional protection priorities.
  - Federal agencies are responsible for enabling or augmenting protection for CIKR that is nationally critical or coordinating the efforts of CIKR 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.
  - The SSAs, in conjunction with sector partners, provide information on the most effective long-term protection

strategies, develop protective programs, and coordinate the implementation of programs for their sectors. For some sectors, this includes the development and sharing of best and effective practices and related criteria, guidance documents, and tools.

  - DHS, in collaboration with the SSAs and other public and private sector partners, serves as the national focal point for the development, implementation, and coordination of risk management approaches and tools and of protective programs and resiliency strategies (including cybersecurity efforts) for those assets that are deemed to be nationally critical.

- **Cost-Effective**: Effective CIKR programs and strategies seek to use resources efficiently by focusing on actions that offer the greatest mitigation of 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 CIKR protection initiatives:

  - Operating with full information: The NIPP describes the mechanisms that enable the use of information regarding threats and corresponding protective actions. These mechanisms include: information sharing; provision of a dedicated communications network; and the use of established, interoperable industry and trade association communications mechanisms.

  - 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 CIKR protection.

  - Matching the underlying economic incentives of each CIKR partner to the full extent possible: The NIPP supports market-based economic incentives wherever possible by relying on CIKR partners to undertake those efforts that are in their own interests and complementing those efforts with additional resources where necessary and appropriate. This coordinated approach builds on existing efforts that have proven to be effective and that are consistent with best business practices, such as owners and operators selecting the measures that are best suited to their particular risk profile and needs.

  - Addressing the public-interest aspects associated with CIKR protection: Risk management actions for CIKR that provide benefits to the public at large go beyond the actions that benefit owners and operators, or even those that benefit the public residing in a particular State, locality, or region. Such additional actions reflect different levels of the public interest—some CIKR are critical to the national economy and to national well-being; some CIKR are critical to a State, locality, or region; some CIKR are critical only to the individual owner/operator or direct customer base. Actions to protect the public's interest that require investment beyond the level that those directly responsible for protection are willing and able to provide must be of sufficient priority to warrant the use of the limited resources that can be provided from public funding or may require regulatory action or appropriate incentives to encourage the private sector to undertake them.

- **Risk-Informed**: Protective programs and resiliency strategies focus on mitigating risk. Associated actions should be designed to allow measurement, evaluation, and feedback based on risk mitigation. This allows owners, operators, and the SSAs to reevaluate risk after the program has been implemented. These programs and strategies use different mechanisms for addressing each element of risk and combine their effects to achieve overall risk mitigation. These mechanisms include:

  - Consequences: Protective programs and resiliency strategies may limit or manage consequences by reducing the possible loss resulting from a terrorist attack or other disaster through redundant system design, backup systems, and alternative sources for raw materials or information.

  - Vulnerability: Protective programs may reduce vulnerability by decreasing the susceptibility to destruction, incapacitation, or exploitation by correcting flaws or strengthening weaknesses in assets, systems, and networks.

  - Threat: Protective programs and resiliency strategies indirectly reduce threat by making assets, systems, or networks less attractive targets to terrorists by lessening their vulnerability and lowering the consequences. As a result, terrorists may be less likely to achieve their objectives and, therefore, less likely to focus on the CIKR in question.

3.5.3 Risk Management Activities, Initiatives, and Reports

DHS, in collaboration with the SSAs and other sector partners, undertakes a number of protective programs, resiliency strategies, initiatives, activities, and reports that support CIKR protection. Many of these are available to or provide resources for CIKR partners. These activities span a wide range of efforts that include, but are not limited to, the following:

IP Vulnerability Assessment Project

The IP Vulnerability Assessment (VA) Project serves as the focal point for strategic planning, coordination, and information sharing in conducting vulnerability assessments of the Nation's Tier 1 and Tier 2 CIKR. Through the development and deployment of a scalable assessment methodology, the VA Project supports the implementation of the NIPP through identifying vulnerabilities, supporting collaborative security planning, and recommending protective measures strategies. IP VA Project initiatives include the BZPP, Site Assistance Visits (SAVs), CRs, and the Computer-Based Assessment Tool (CBAT). The VA Project provides vulnerability assessment methodologies that enhance DHS's and CIKR stakeholders' ability to prevent, protect, and respond to terrorist attacks and all-hazards incidents. The VA Project brings together: Federal, State, local, tribal, and territorial governments; local law enforcement; emergency responders; and CIKR owner and operators to conduct assessments to identify critical assets, vulnerabilities, consequences, and protective measures and resiliency strategies. The VA Project also provides analysis of CIKR facilities to include: potential terrorist actions for an attack; the consequences of such an attack; and the integrated preparedness and response capabilities of Federal, State, local, tribal, and territorial and private sector partners. The results are used to enhance the overall CIKR protection posture at the facility, community, and regional levels using short-term enhancements and long-term risk-informed investments in training, processes, procedures, equipment, and resources.

- **Buffer Zone Protection Program**: A Federal grant program designed to provide resources to State and local law enforcement to enhance the protection of a given critical facility.
- **Assistance Visits**: Facility security assessments jointly conducted by a federally led team and facility owners and operators that are designed to facilitate vulnerability identification and mitigation discussions with individual owners and operators.
- **Training Programs**: Training programs are designed to provide CIKR partners with a source from which they can obtain specialized training to enhance CIKR protection. Subject matter, course length, and location of training can be tailored to the partner's needs.
- **Control System Security**: DHS 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 CIKR sectors.
- **Multi-Jurisdictional Improvised Explosive Device Security Plans**: DHS assists high-risk urban environments with developing thorough IED security plans that efficiently integrate assets and capabilities from multiple jurisdictions and emergency services disciplines. The plan that results from this process can help determine what actions are necessary to enhance IED prevention and the protection capabilities of the multi-jurisdictional area, which ultimately culminates in the development of a NRF- and National Incident Management System (NIMS)-compliant multi-jurisdictional plan.
- **Protective Security Advisor (PSA) Program**: DHS CIKR protection and vulnerability assessment specialists are assigned as liaisons between DHS and the CIKR protection community at the State, local, and private sector levels in geographical areas representing major concentrations of CIKR across the United States. PSAs are responsible for sharing risk information and providing technical assistance to local law enforcement and owners and operators of CIKR within their respective areas of responsibility. The PSA Duty Desk serves as the conduit among the PSAs, DHS, and other CIKR partners to facilitate, on a 24/7 basis, coordination and collaboration during steady-state and incident operations.

Protective Security Advisors

The mission of the PSAs is to represent DHS and IP in local communities throughout the United States. PSAs work with State HSAs, acting as liaisons among: DHS; the private sector; and Federal, State, local, tribal, and territorial entities and serving as DHS locally based critical infrastructure protection specialists. PSAs provide support to officials responsible for special events planning and exercises, and provide real-time information on facility significance and protective measures to facility owners and operators, as well as State and local representatives. PSAs assist and facilitate IP efforts to identify, assess, monitor, and minimize risk to CIKR at the State, local, and regional levels.

As a result of their national "footprint" across the United States, PSAs are often the first department personnel to provide support for emergent incidents. Consequently, PSAs are uniquely able to provide early situational awareness to DHS and IP leadership during an incident or contingency operations. During natural disasters and contingencies, PSAs deploy to State and local Emergency Operations Centers (EOCs) and SLFCs to provide situational awareness and facilitate information exchange to and from the field. During incidents, upon designation by the Assistant Secretary of Infrastructure Protection, PSAs perform as Infrastructure Liaisons (ILs) at Joint Field Offices (JFOs) in support of the Principal Federal Officials (PFOs) and Federal Coordinating Officers (FCOs) under the NRF.

A detailed discussion of DHS-supported programs is provided in appendix 3B.

The SSAs and other Federal departments and agencies also oversee programs, initiatives, and activities that support CIKR protection and resiliency. Many of these are also available to or provide resources for CIKR partners. Examples include:

- The Department of Veterans Affairs created a methodology also used by the Smithsonian Institution and adapted by Federal Emergency Management Agency (FEMA) Manual 452, Risk Management: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings, to assess the risk to and mitigation for hundreds of buildings and museums.
- DOT manages a Pipeline Safety grant program that supports efforts to develop and maintain State natural gas, liquefied natural gas, and hazardous liquid pipeline safety programs.
- Other risk management activities include developing and providing informational reports, such as the DHS Characteristics of Common Vulnerabilities Reports and the Indicators of Terrorist Activity Reports, which are available to all State and territorial homeland security offices. In addition to threat and vulnerability information, informational reports also include best practices for protection measures. One report in particular, a part of FEMA's Risk Management Series, addresses the protection of buildings and is applicable across sectors.

Enhanced Critical Infrastructure Protection (ECIP) Program

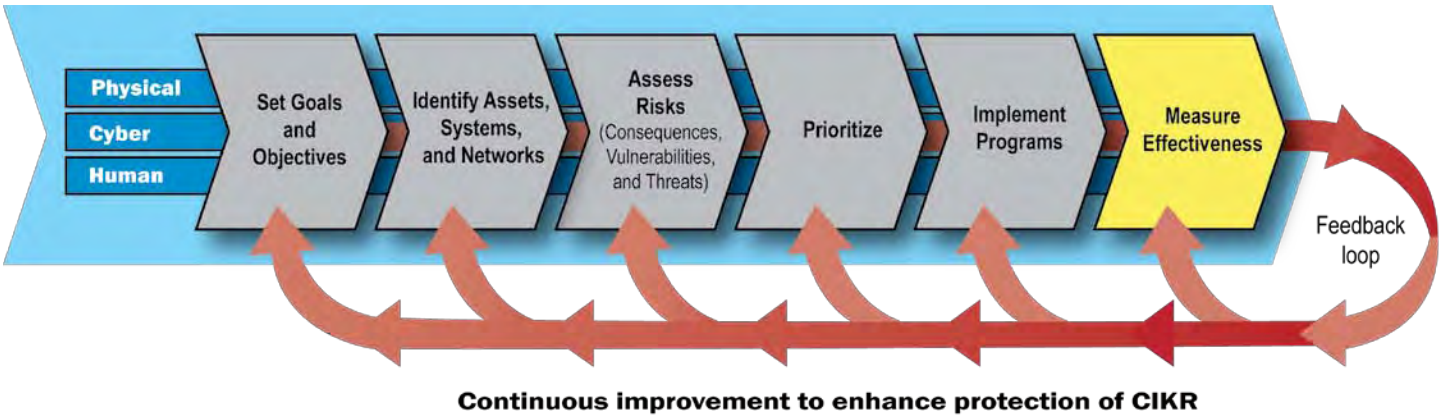
PSAs were directed to form partnerships with the owners and operators of the Nation's Tier 1 and Tier 2 CIKR and conduct site visits (ECIP visits) for all of these assets. PSAs coordinate site visits with the SSAs, owners and operators, HSAs, FBI, local law enforcement (LLE), and other CIKR partners, as necessary. During the visit, PSAs document information on the facility's current CIKR protection posture and overall security awareness. The primary goals for ECIP site visits are to:

- Inform facility owners and operators of the importance of their facilities as an identified high-priority CIKR and the need to be vigilant in light of the ever-present threat of terrorism;
- Identify protective measures currently in place at Tier 1 and Tier 2 facilities, provide comparisons of CIKR protection postures across like assets, and track the implementation of new protective measures; and
- Enhance existing relationships between Tier 1/Tier 2 facility owners and operators, DHS, and various Federal, State, local, tribal, and territorial partners in order to:
  - Provide increased situational awareness regarding potential threats;
  - Maintain an indepth knowledge of the current CIKR protection posture at each facility; and
  - Provide a known and available Federal resource to facility owners and operators.

3.6 Measure Effectiveness

The use of performance metrics is a critical step in the NIPP risk management process to enable DHS and the SSAs to objectively and quantitatively assess improvements in CIKR protection and resiliency at the sector and national levels. While the results of risk analyses outlined in section 3.3 help sectors set priorities, performance metrics allow NIPP partners to track progress against these priorities. The metrics provide a basis for DHS and the SSAs to establish accountability, document actual performance, facilitate diagnoses, promote effective management, and provide a feedback mechanism to decisionmakers.

Figure 3-7: NIPP Risk Management Framework: Measure Effectiveness



3.6.1 NIPP Metrics Types and Progress Indicators

3.6.1.1 Outcome Metrics

The focus of the NIPP metrics program is to track progress toward a strategic goal by measuring beneficial results or outcomes. The key to NIPP performance management is to align outcome metrics to sector priorities. The 18 sectors are diverse, operate in every State, and affect every level of government. As a result, NIPP priorities and many NIPP metrics will vary from sector to sector. All NIPP metrics must be specific and clear as to what they are measuring, practical or feasible in that the needed data are available, and built on objectively measured data.

In addition to outcome metrics, other information will be utilized, such as output data and descriptive data.

- *Output (or Process) Data* are used to gauge whether specific activities were performed as planned, track the progress of a task, or report on the output of a process. Output data show progress toward performing the activities necessary to achieve CIKR protection goals and can serve as leading indicators for outcome measures. They also help build a comprehensive picture of CIKR protection status and activities. Examples include the number of protective programs implemented in a fiscal year, percentage of sector organizations exchanging CIKR information, and the level of response to a data call for asset information.
- *Descriptive Data* are used to understand sector resources and activities, but do not reflect CIKR protection performance. Examples include: a narrative description of progress; the number of facilities in a jurisdiction; the population resident or working in the area affected by an incident; and the number of suppliers in an infrastructure service provider's supply chain.

NIPP metrics are evolving from the current focus on descriptive and output data to a focus on outcome metrics. Descriptive and output data have been critical during the initial implementation of the NIPP in order to closely track the progress of the sectors in building key NIPP elements, such as the SSPs and GCCs/SCCs. The next stage of NIPP implementation will concentrate on working with the sectors to identify and track outcome metrics that are aligned to sector priorities and provide NIPP partners with a more comprehensive assessment of the success of CIKR protection efforts.

3.6.1.2 NIPP Metrics Progress Indicators

NIPP outcome metrics and output/descriptive data will be identified and reported in two ways—the National Coordinator Progress Indicator and Sector Progress Indicators:

The National Coordinator Progress Indicator describes IP efforts to support NIPP- and SSP-related activities.

Sector Progress Indicators collectively describe the progress made by each sector and the effectiveness of different activities within the CIKR sectors.

Both types of progress indicators will have certain common features. They will contain a limited number of prioritized metrics and data that are aligned to sector priorities. Outcome metrics will be given the most importance, but some process and descriptive data may be included. Collectively, these metrics and data will provide a holistic picture of the health and effectiveness of the national and sector CIKR efforts and will help drive future investment and resource decisions.

3.6.1.3 Qualitative Information

Although not considered metrics, the NIPP also provides mechanisms for qualitative feedback that can be applied to augment and improve the effectiveness and efficiency of public and private sector CIKR protection and resiliency programs. DHS works with CIKR partners to identify and share lessons learned and best practices for all aspects of the risk management process. DHS also works with the SSAs to share relevant input from sector partners and other sources that can be used as part of the national effort to continuously improve CIKR protection and resiliency.

3.6.2 Gathering Performance Information

DHS works with the SSAs and sector partners to gather the information necessary to measure the level of performance associated with the progress indicators. Given the inherent differences in CIKR sectors, a one-size-fits-all approach to gathering this information is not appropriate. One of the available resources to support information gathering is the PSA Program through the ECIP/Infrastructure Survey Tool. The PSAs can be particularly helpful in gathering information at individual facilities or assets when different CIKR protection initiatives are implemented. This information can be used independently or combined with that of other assets, as well as with data on systems and networks that may not be amenable to physical inspection.

DHS also works with the SSAs and sector partners to determine the appropriate measurement approach to be included in the sector's SSP and to help ensure that partners engaged with multiple sectors or in cross-sector matters are not subject to unnecessary redundancy or conflicting guidance in information collection. Information collected as part of this effort is protected as discussed in detail in chapter 4.

3.6.3 Assessing Performance and Reporting on Progress

HSPD-7 requires each SSA to provide the Secretary of Homeland Security with an annual report on their efforts to identify, prioritize, and coordinate the protection of CIKR in their respective sectors. The reports are due no later than June 1 of each year. The SSAs work in close collaboration with sector partners, their respective SCCs and GCCs, and other organizations in developing this report. DHS and SSAs work in close collaboration to assess progress made toward goals in each sector based on these reports.

The National Annual Report currently includes similar reports for the SLTTGCC and the RCCC as appendixes. Additional appendixes to the current National Annual Report address the year's accomplishments for IP, the Office of Cybersecurity & Communications, the Tier 1 and Tier 2 Program, and the NISAC.

DHS compiles all of these reports into a national cross-sector report that describes annual progress toward CIKR protection goals on a national basis and makes recommendations to the EOP for prioritized resource allocation across the Federal Government to meet national CIKR protection requirements. A more detailed discussion of the national resource allocation process for CIKR protection is included in chapter 7.

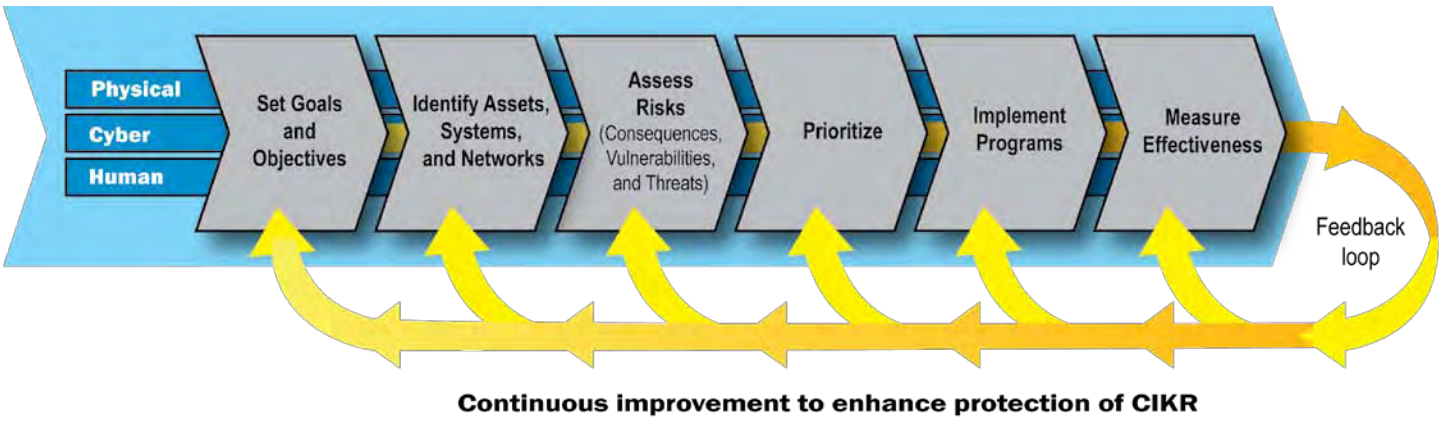
In addition to these annual reports, the SSAs regularly update their measurements of CIKR status and protection levels to support DHS status tracking and comprehensive inventory updating. By maintaining a regularly updated knowledge base, DHS is able to quickly compile real-time CIKR status and protection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

3.7 Using Metrics and Performance Measurement for Continuous Improvement

By using NIPP metrics to evaluate the effectiveness of efforts to achieve sector priorities, CIKR partners adjust and adapt the Nation's CIKR 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 are used to focus attention on areas of CIKR protection that warrant additional government resources or other changes through an analysis of gaps and priorities for protective programs at both the national and sector levels. If an evaluation of the effectiveness of efforts to achieve priorities using NIPP metrics reveals that there is insufficient progress, DHS and its CIKR partners will undertake actions to focus efforts on addressing these particular gaps or improvement opportunities.

In addition to supporting the evaluation of progress against sector priorities, metrics can also serve as a feedback mechanism for other parts of the NIPP risk management framework. The metrics can inform progress against the broader sector goals (see section 3.1). Metrics can also provide analysts with information to adjust their risk assessments (see section 3.3). For instance, metrics indicate the effectiveness of protective programs and the extent to which these programs are mitigating risks. Finally, metrics can also inform the prioritization process (see section 3.4), as this information can assist decisionmakers in identifying effective ways to achieve desired outcomes.

Figure 3-8: NIPP Risk Management Framework: Feedback Loop for Continuous Improvement of CIKR Protection



4. Organizing and Partnering for CIKR Protection

The enormity and complexity of the Nation's CIKR, the distributed character of our national protective architecture, and the uncertain nature of the terrorist threat and manmade or natural hazards make the effective implementation of protection and resiliency efforts a great challenge. To be effective, the NIPP must be implemented using organizational structures and partnerships committed to sharing and protecting the information needed to achieve the NIPP goal and supporting objectives described in chapter 1. DHS, in close collaboration with the SSAs, is responsible for overall coordination of the NIPP partnership organization and information-sharing network.

4.1 Leadership and Coordination Mechanisms

The coordination mechanisms described below establish linkages among CIKR protection efforts at the Federal, State, regional, local, tribal, territorial, and international levels, as well as between public and private sector partners. In addition to direct coordination, the structures described below provide a national framework that fosters relationships and facilitates coordination within and across CIKR sectors:

- **National-Level Coordination**: IP facilitates overall development of the NIPP and the SSPs, provides overarching guidance, and monitors the full range of associated coordination activities and performance measures. IP will support, not duplicate, SSA coordination, protection, or other risk reduction capabilities. Chapter 2 details specific roles for DHS.
- **Sector Partnership Coordination**: The CIKR Cross-Sector Council; the Government Cross-Sector Council (made up of two subcouncils—the NIPP Federal Senior Leadership Council (FSLC) and the SLTTGCC); and individual SCCs and GCCs create a structure through which representative groups from Federal, State, local, and tribal governments and the private sector can collaborate and develop consensus approaches to CIKR protection.
- **Regional Coordination**: Regional partnerships, groupings, and governance bodies such as the Great Lakes Partnership, the All-Hazards Consortium, the Pacific NorthWest Economic Region, and the Southeast Regional Research Initiative enable CIKR protection coordination 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 an aggregation of high-risk targets, urban areas, or cross-sector groupings. They facilitate enhanced coordination among jurisdictions within a State where CIKR cross multiple jurisdictions, and help sectors coordinate with multiple States that rely on a common set of CIKR. They also are organized to address common approaches to a wide variety of natural or manmade hazards. The RCCC was established in 2008 to help enhance the engagement of regionally based partners and to leverage the CIKR protection activities and resiliency strategies that they lead.

- **International Coordination**: The United States-Canada-Mexico Security and Prosperity Partnership; the North Atlantic Treaty Organization's (NATO's) Senior Civil Emergency Planning Committee; certain government councils, such as the CFIUS; the CFDI; and consensus-based nongovernmental or public-private organizations, such as the global Forum of Incident Response and Security Teams (FIRST), enable a range of CIKR protection coordination activities associated with established international agreements.

4.1.1 National-Level Coordination

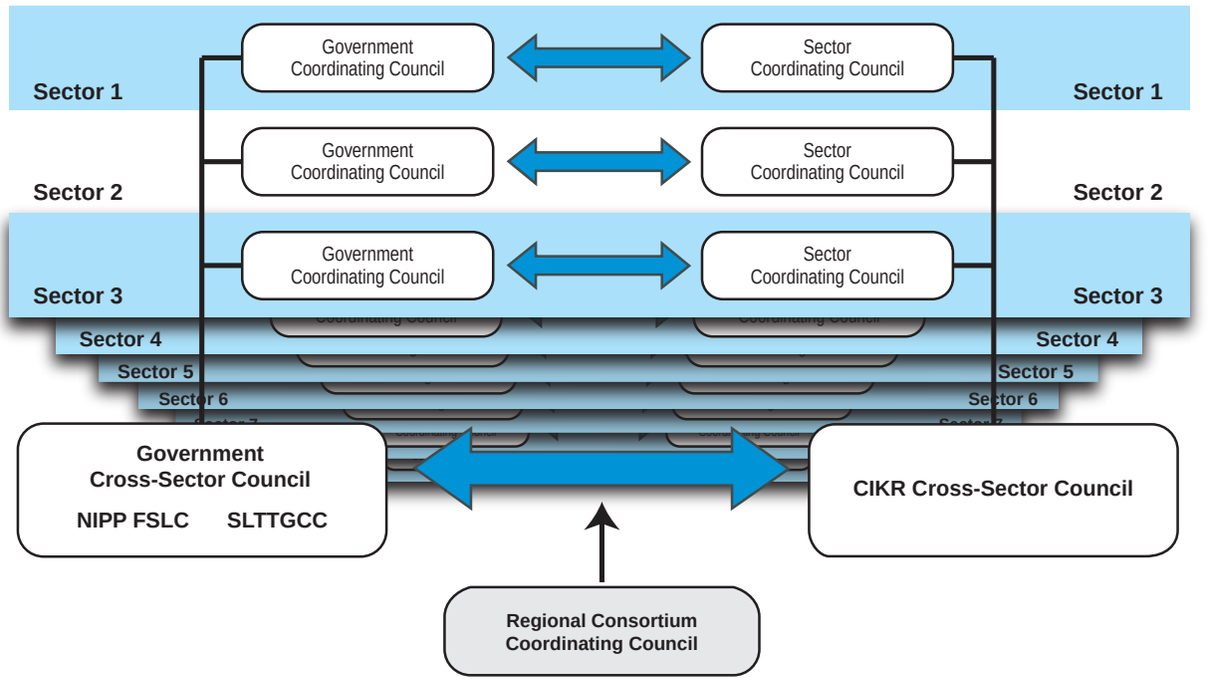
Respecting the SSA's responsibilities as the sector lead, DHS, in collaboration with the SSAs and the GCCs, monitors the coordination and integration of national-level CIKR protection activities through IP. In support of CIKR partner coordination, DHS:

- Leads, integrates, and coordinates the execution of the NIPP, in part by acting as a central clearinghouse for the information-sharing, reporting, and coordination activities of the individual sector governance structures;
- Facilitates the development and ongoing support of governance and coordination structures or models;
- Facilitates NIPP revisions and updates using a comprehensive national review process;
- Ensures that effective policies, approaches, guidelines, and methodologies regarding partner coordination are developed and disseminated to enable the SSAs and other partners to carry out NIPP responsibilities;
- Facilitates the development of risk, risk-informed, and criticality-based assessments and prioritized lists of CIKR;
- Facilitates the sharing of CIKR prioritization and protection-related best practices and lessons learned;
- Facilitates participation in preparedness activities, planning, readiness exercises, and public awareness efforts; and
- Ensures cross-sector coordination with the SSAs to avoid conflicting guidance, duplicative requirements, and reporting.

4.1.2 Sector Partnership Coordination

The goal of NIPP-related organizational structures, partnerships, and information-sharing networks is to establish the context, framework, and support for activities required to implement and sustain the national CIKR protection effort. DHS, in collaboration with the SSAs and sector partners, issues coordinated guidance on the framework for CIKR public-private partnerships, as well as metrics to measure their effectiveness.

Figure 4-1: Sector Partnership Model



The NIPP relies on a partnership model, illustrated in figure 4-1, as the primary organizational structure for coordinating CIKR efforts and activities. The NIPP partnership model encourages formation of SCCs and GCCs as described below. DHS also provides guidance, tools, and support to enable these groups to work together to carry out their respective roles and responsibilities. SCCs and corresponding GCCs work in tandem to create a coordinated national framework for CIKR protection and resiliency within and across sectors. The sector partnership model facilitates the integration of all partners into CIKR planning and operational activities to help ensure a collaborative approach to CIKR protection.

4.1.2.1 CIKR Cross-Sector Council

Cross-sector issues and interdependencies are addressed among the SCCs through the CIKR Cross-Sector Council, which comprises the leadership of each of the SCCs. The Partnership for Critical Infrastructure Security provides this representation with support from DHS's CIKR Executive Secretariat. The partnership coordinates cross-sector initiatives to support CIKR protection by identifying legislative issues that affect such initiatives and by raising awareness of issues in CIKR protection. The primary activities of the CIKR Cross-Sector Council include:

- Providing senior-level, cross-sector strategic coordination through partnership with DHS and the SSAs;
- Identifying and disseminating CIKR protection best practices across the sectors;
- Participating in coordinated planning efforts related to the development, implementation, and revision of the NIPP and the SSPs or aspects thereof; and
- Coordinating with DHS to support efforts to plan and execute the Nation's CIKR protection mission.

4.1.2.2 Government Cross-Sector Council

Cross-sector issues and interdependencies between the GCCs will be addressed through the Government Cross-Sector Council, which comprises two subcouncils—the NIPP FSLC and the SLTTGCC:

- **NIPP Federal Senior Leadership Council**: The objective of the NIPP FSLC is to facilitate enhanced communications and coordination between and among Federal departments and agencies with a role in implementing the NIPP and HSPD-7. The council's primary activities include:
  - Forging consensus on CIKR risk management strategies;
  - Evaluating and promoting implementation of risk management-based CIKR programs;
  - Coordinating strategic issues and issue management resolution among Federal departments and agencies, and State, regional, local, tribal, and territorial partners;
  - Advancing collaboration within and across sectors;
  - Advancing collaboration with the international community;
  - Participating in planning efforts related to the development, implementation, update, and revision of the NIPP and the SSPs or aspects thereof; and
  - Evaluating and reporting on the progress of Federal CIKR protection activities.
- **State, Local, Tribal, and Territorial Government Coordinating Council**: The SLTTGCC serves as a forum to ensure that State, local, and tribal homeland security partners are fully integrated as active participants in national CIKR protection efforts and to provide an organizational structure to coordinate across jurisdictions on State and local government-level CIKR protection guidance, strategies, and programs. The SLTTGCC will provide the State, local, tribal, or territorial perspective or feedback on a wide variety of CIKR issues. The primary functions of the SLTTGCC include the following:
  - Providing senior-level, cross-jurisdictional strategic communications and coordination through partnership with DHS, the SSAs, and CIKR owners and operators;
  - Participating in planning efforts related to the development, implementation, update, and revision of the NIPP and SSPs or aspects thereof;
  - Coordinating strategic issues and issue management resolution among Federal departments and agencies, and State, local, tribal, and territorial partners;
  - Coordinating with DHS to support efforts to plan, implement, and execute the Nation's CIKR protection mission; and
  - Providing DHS with information on State-, local-, tribal-, and territorial-level CIKR protection initiatives, activities, and best practices.

The cross-sector bodies described in sections 4.1.2.1 and 4.1.2.2 will convene in joint session and/or working groups, as appropriate, to address cross-cutting CIKR protection issues. The NIPP-related functions of the cross-sector bodies include activities to:

- Provide or facilitate coordination, communications, and strategic-level information sharing across sectors and between and among DHS, the SSAs, the GCCs and other

supporting Federal departments and agencies, and other public and private sector 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 information-sharing, planning, and risk management activities, as appropriate; and
- Provide input to the government on R&D efforts that would benefit multiple sectors.

4.1.2.3 Sector Coordinating Councils

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

The SCCs enable owners and operators to interact on a wide range of sector-specific strategies, policies, activities, and issues. The SCCs serve as principal sector policy coordination and planning entities. Sectors also rely on ISACs, or other information-sharing mechanisms, which provide operational and tactical capabilities for information sharing and, in some cases, support for incident response activities. (A more detailed discussion of ISAC roles and responsibilities is included in section 4.2.7.)

The primary functions of an SCC include the following:

- Represent a primary point of entry for government into the sector for addressing the entire range of CIKR protection activities and issues for that sector;
- Serve as a strategic communications and coordination mechanism between CIKR owners, operators, and suppliers, and, as appropriate, with the government during emerging threats or response and recovery operations, as determined by the sector;
- Identify, implement, and support the information-sharing capabilities and mechanisms that are most appropriate for the sector. The ISACs may perform this role if so designated by the SCC;
- Participate in planning efforts related to the development, implementation, update, and revision of the SSPs and review of the Sector Annual Reports;
- Facilitate inclusive organization and coordination of the sector's policy development regarding CIKR protection planning and preparedness, exercises and training, public awareness, and associated plan implementation activities and requirements;
- Advise on the integration of Federal, State, local, and regional planning with private sector initiatives; and
- Provide input to the government on sector R&D efforts and requirements.

The SCCs are encouraged to participate in efforts to develop voluntary consensus standards to ensure that sector perspectives are included in standards that affect CIKR protection.[7]

4.1.2.4 Government Coordinating Councils

A GCC is formed as the government counterpart for each SCC to enable interagency and cross-jurisdictional coordination. The GCC comprises representatives from across various levels of government (Federal, State, local, or tribal), as appropriate to the operating landscape of each individual sector. Each GCC is co-chaired by a representative from the designated SSA with responsibility for ensuring appropriate representation on the GCC and providing cross-sector coordination with State, local, and tribal governments. Each GCC is co-chaired by the DHS Assistant Secretary for Infrastructure Protection or his/her designee.

The GCC coordinates strategies, activities, policy, and communications across governmental entities within each sector. The primary functions of a GCC include the following:

- Provide interagency strategic communications and coordination at the sector level through partnership with DHS, the SSA, and other supporting agencies across various levels of government;
- Participate in planning efforts related to the development, implementation, update, and revision of the NIPP and the SSPs;

[7] Voluntary consensus standards are developed or adopted by voluntary consensus standards bodies, both domestic and international. These organizations plan, develop, establish, or coordinate standards through an agreed-upon procedure that relies on consensus, although not necessarily on unanimity. Federal law encourages Federal participation in these bodies to increase the likelihood that standards meet both public and private sector needs. Examples of other standards that are distinct from voluntary consensus standards include non-consensus standards, industry standards, company standards, or de facto standards developed in the private sector but not in the full consensus process, standards that are unique to government and developed by government for its own uses, and standards mandated by law.

- Coordinate strategic communications and discussion and resolution of issues among government entities within the sector; and
- Coordinate with and support the efforts of the SCC to plan, implement, and execute the Nation's CIKR protection mission.

4.1.2.5 Regional Consortium Coordinating Council

The RCCC brings together representatives of regional partnerships, groupings, and governance bodies to enable CIKR protection coordination among CIKR partners within and across geographical areas and sectors.

4.1.2.6 Critical Infrastructure Partnership Advisory Council (CIPAC)

CIPAC directly supports the sector partnership model by providing a legal framework that enables members of the SCCs and GCCs to engage in joint CIKR protection-related discussions. CIPAC serves as a forum for government and private sector partners to engage in a broad spectrum of activities, such as:

- Planning, coordination, implementation, and operational issues;
- Implementation of security and preparedness programs;
- Operational activities related to CIKR protection, including incident response and recovery; and
- Development and support of national policies and plans, including the NIPP and the SSPs.

CIPAC membership consists of private sector CIKR owners and operators, or their representative trade or equivalent associations, from the respective sector's recognized SCC, and representatives of Federal, State, local, and tribal governmental entities (including their representative trade or equivalent associations) that make up the corresponding GCC for each sector. DHS published a Federal Register Notice on March 24, 2006, announcing the establishment of CIPAC as a FACA-exempt body, pursuant to section 871 of the Homeland Security Act.

4.1.3 Regional Coordination and the Partnership Model

Regional partnerships, organizations, and governance bodies enable CIKR protection coordination among CIKR partners within and across certain geographical areas, as well as 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 interstate or intrastate, vary widely in terms of mission, composition, and functionality. Regardless of the variations, these organizations provide structures at the strategic and/or operational levels that help address cross-sector CIKR planning and protection program implementation. They may also provide enhanced coordination among jurisdictions within a State where CIKR cross multiple jurisdictions and help sectors coordinate with multiple States that rely on a common set of CIKR. In some instances, State Homeland Security Advisors may serve as focal points for regional initiatives and provide linkages between the regional organizations and the sector partnership model. Based on the nature or focus of the regional initiative, these organizations may link into the sector partnership model, as appropriate, through the individual SCCs or GCCs or cross-sector councils, or more broadly through the RCCC.

4.1.4 International CIKR Protection Cooperation

Many CIKR assets, systems, and networks, both physical and cyber, are interconnected with a global infrastructure that has evolved to support modern economies. Each of the CIKR sectors is linked in varying degrees to global energy, transportation systems, telecommunications, cyber, and other infrastructure. This global system creates benefits and efficiencies, but also brings interdependencies, vulnerabilities, and challenges in the context of CIKR protection. The Nation's safety, security, 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 CIKR protection coordination and cooperation is focused on:

- Instituting effective cooperation with international CIKR partners, as well as high-priority cross-border protection programs. Specific protective actions are developed through the sector planning process and specified in the SSPs and the annual CFDI Action Plan;
- Implementing current agreements and instruments that affect CIKR protection;
- Identifying infrastructure located outside the United States that if disrupted or destroyed would lead to loss of life in the United States, or critically affect the Nation's economic, industrial, or defensive capabilities; and

- Addressing cross-sector and global issues such as cybersecurity and foreign investment.

International CIKR protection activities require coordination with the DOS and appropriate SSAs and must be designed and implemented to benefit the United States and its international partners.

CIKR protection may be affected by foreign investment and ownership of sector assets. This issue is monitored at the Federal level by the CFIUS. The committee provides a forum for assessing the impact of proposed foreign investments on CIKR protection, monitoring to ensure compliance with agreements that result from CFIUS rulings, and supporting executive branch reviews of telecommunications applications to the Federal Communications Commission (FCC) from foreign entities to assess if they pose any national security threat to CIKR (see appendix 1B.4.2).

4.1.4.1 Cooperation With International Partners

DHS, in coordination with the appropriate SSAs, other Federal agencies, and the Department of State (DOS), works with international partners and other entities involved in the international aspects of CIKR protection to exchange experiences, share information, and develop a cooperative environment to materially improve U.S. CIKR protection. DHS, the DOS, and the SSAs work with foreign governments to identify international interdependencies, vulnerabilities, and risk-mitigation strategies, and through international organizations, such as the Group of Eight (G8), NATO, the European Union, the Organization of American States (OAS), and the Organisation for Economic Co-operation and Development (OECD), to enhance CIKR protection. Forums such as the International Maritime Organization (IMO), a specialized agency of the United Nations, cooperate with a host of partners to govern international shipping; develop and maintain a regulatory framework for shipping; address safety and environmental concerns; legal matters and others. The IMO is based in the United Kingdom and has 168 member states.

While the SSAs and owners and operators generally are responsible for developing CIKR protection programs to address risks that arise from or include international sources or considerations, DHS manages specific programs to enhance the cooperation and coordination needed to address the unique challenges and opportunities posed by the international aspects of CIKR protection. The following DHS efforts augment, but do not supersede or replace, the activities and programs of other Federal agencies or other NIPP partners.

- **Critical Foreign Dependencies Initiative**: In accordance with the NIPP, the Federal Government created a comprehensive inventory of infrastructure located outside the United States that if disrupted or destroyed would lead to loss of life in the United States or critically affect the Nation's economy or national security. In response to this requirement, DHS worked with the DOS to develop the CFDI, a process designed to ensure that the resulting classified National Critical Foreign Dependencies List is inclusive, representative, and leveraged in a coordinated and responsible manner.
- **International Outreach Program**: DHS, in cooperation with the DOS and other Federal agencies, carries out international outreach activities to engage foreign governments and international/multinational organizations to promote a global culture of CIKR protection. These outreach activities enable international cooperation and engage constituencies that often do not traditionally address CIKR protection. This outreach encourages the development and adoption of best practices, training, and other programs designed to improve the protection of U.S. CIKR overseas, as well as the reliability of international CIKR on which this country depends. Other Federal, State, local, tribal, and private sector entities also engage in international outreach that may be related to CIKR risk mitigation in situations where they work directly with their foreign counterparts.
- **The National Exercise Program (NEP)**: DHS provides overarching coordination for the NEP to ensure the Nation's readiness to respond in an all-hazards environment and to practice and evaluate the steady-state protection plans and programs put in place by the NIPP. The NEP provides opportunities through exercises for international partners to engage with Federal, State, and local departments and agencies to address cooperation and cross-border issues, including those related to CIKR protection. DHS and other CIKR partners also participate in exercises sponsored by international partners.
- **National Cyber Exercises**: DHS and its partners conduct exercises to identify, test, and improve coordination of the cyber incident response community, including Federal, State, regional, local, tribal, and international governmental entities, as well as private sector corporations and coordinating councils.

Where applicable, DHS encourages the use of PCII protections to safeguard private sector CIKR information when sharing it with international partners. The PCII Program will solicit the submitter's express permission before sharing the submitter's proprietary CIKR information with international partners.

4.1.4.2 Implementing Current Agreements

DHS, the SSAs, and other Federal agencies have entered into agreements with international partners, including bilateral

and multilateral partnerships, with the assistance of the DOS. The key partners involved in existing agreements include:

- **Canada and Mexico**: CIKR interconnectivity between the United States and its immediate neighbors makes the borders virtually transparent. Electricity, natural gas, oil, roads, rail, food, water, minerals, and finished products cross our borders with Canada and Mexico as a routine component of commerce and infrastructure operations. The importance of this trade, and the infrastructure that support it, was highlighted after the terrorist attacks of September 11, 2001, nearly closed both borders. The United States entered into the 2001 Smart Border Declaration with Canada and the 2002 Border Partnership Declaration with Mexico, in part, to address bilateral CIKR issues. In addition, the 2005 Security and Prosperity Partnership of North America (SPP) established a common approach to security to protect North America from external threats, prevent and respond to threats, and further streamline the secure and efficient movement of legitimate, low-risk traffic across the shared borders.
- **United Kingdom**: The United Kingdom is a close ally of the United States that has extensive experience in counterterrorism and CIKR protection. The United Kingdom has developed substantial expertise in law enforcement and intelligence systems, and in the protection of commercial facilities based on its counterterrorism experience. Like the United States, most of the critical infrastructure in the United Kingdom is privately owned. The government of the United Kingdom developed an effective, sophisticated system to manage public-private partnerships. DHS formed a Joint Contact Group (JCG) with the United Kingdom that brings officials into regular, formal contact to discuss and resolve a range of bilateral homeland security issues.
- **The Group of Eight**: Since September 11, 2001, the infrastructure in several G8 countries has been exploited and used to inflict casualties and fear. As a result, G8 partners underscored their determination to combat all forms of terrorism and to strengthen international cooperation. To that end, within the G8 context, the United States spearheaded various CIKR protection initiatives in 2007 and 2008. The first project focused on G8 delegation nation security planning best practices, vulnerability assessment methodologies, and threat assessments for critical energy infrastructure. The second project focused on Chemical Sector infrastructure protection activities, a timely subject given the release of the CFATS in the United States the previous year. These projects have increased the baseline understanding of the measures underway, as well as the CIKR protection capabilities of each G8 member nation. The G8 provides an effective forum for member nations to work together to reduce global risks to CIKR by sharing best practices and methodologies and to understand common threats. Future projects related to critical infrastructure protection within the G8 will address issues related to interdependencies within and across critical infrastructure systems.
- **Asia-Pacific Economic Cooperation (APEC)**: This group is responding to the terrorist threat by pursuing several practical counterterrorist initiatives that are intended to prevent the movement of funds, goods, and people involved in terrorist activities, while at the same time ensuring that the legitimate cross-border movement of goods and people is not impeded. APEC established the Counterterrorism Task Force to assist economies in identifying, assessing, and coordinating counterterrorism capacity building. Other APEC measures include the Secure Trade in the APEC Region (STAR) initiative, under which members have developed measures to secure cargo, protect people in transit, strengthen the security of ships and ports, improve airline passenger systems and crew safety, and strengthen border controls.
- **North Atlantic Treaty Organization**: NATO addresses CIKR protection issues through the Senior Civil Emergency Planning Committee, the senior policy and advisory body to the North Atlantic Council on civil emergency planning and disaster relief matters. The committee is responsible for policy direction and coordination of planning boards and committees in the NATO environment. It has developed considerable expertise that applies to CIKR protection and has planning boards and committees covering ocean shipping, inland surface transport, civil aviation, food and agriculture, industrial preparedness, civil communications planning, civil protection, and civil-military medical issues.
- **European Union**: The United States is engaged in a number of CIKR protection activities with the European Union, including those related to advising the European Union on CIKR risk analysis and management, writ large, as well as counter-explosive device activities. The European Commission is in the process of implementing the European Programme for Critical Infrastructure Protection (EPCIP). This program will affect all 27 nations in the European Union, as well as others in the Euro-Zone that elect to participate. EPCIP will initially focus on the Energy and Transport sectors, with expanded focus on the Telecommunications, Financial, and Chemical sectors in coming years. The United States has engaged the EPCIP leadership for the purpose of offering the assistance necessary to support the implementation of the program, with the ultimate goal of enhancing CIKR protection activities across the board. Furthermore, through both IP and the Science and Technology Directorate, DHS works with the Bureau of Diplomatic Security and

the Office of the Coordinator for Counterterrorism at DOS, DOJ, and the FBI to conduct workshops, seminars, and exercises with the European Union on countering terrorist use of explosive devices. These two activities serve as models for U.S. engagement with the European Union on joint CIKR protection activities.

4.1.4.3 Approach to International Cybersecurity

The United States proactively integrates its: intelligence capabilities to protect the country from cyber attack; its diplomatic outreach, advocacy, and operational capabilities to build awareness, preparedness, capacity, and partnerships in the global community; and its law enforcement capabilities to combat cyber crime wherever it originates. The private sector, international industry associations, and companies with global interests and operations also are engaged in addressing cybersecurity internationally. For example, the U.S.-based Information Technology Association of America participates in international cybersecurity conferences and forums, such as the India-based National Association for Software and Service Companies Joint Conference. These efforts require interaction between policy and operations functions to coordinate national and international activity that is mutually supportive around the globe:

- **International Cybersecurity Outreach**: DHS, in cooperation with the DOS, other Federal departments and agencies, and the private sector, engages in multilateral and bilateral discussions to further international computer security awareness and policy development, as well as incident response team information-sharing and capacity-building objectives. DHS engages in bilateral discussions on cybersecurity issues with various international partners, such as India, Italy, Japan, and Norway. DHS also works with international partners in multilateral and regional forums to address cybersecurity and critical infrastructure information protection. For example, the APEC Telecommunications Working Group recently engaged in a capacity-building program to help member countries develop computer emergency response teams. The OAS has approved a framework proposal by its Cyber Security Working Group to create an OAS regional computer incident response contact network for information sharing and capacity building. Multilateral collaboration to build a global culture of security includes participation in the OECD, the G8, and the United Nations. Many of these countries and organizations have developed mechanisms for engaging the private sector in dialogue and program efforts.
- **Collaboration on Cyber Crime**: The U.S. outreach strategy for comprehensive cyber laws and procedures draws on the Council of Europe Convention on Cyber Crime, as well as: (1) the G8 High-Tech Crime Working Group's principles for fighting cyber crime and protecting critical information infrastructure, (2) the OECD guidelines on information and network security, and (3) the United Nations General Assembly resolutions based on the G8 and OECD efforts. The goal of this outreach strategy is to encourage foreign governments and regional organizations to join the United States in efforts to protect internationally interconnected systems.
- **Collaborative Efforts for Cyber Watch Warning and Incident Response**: The United States works with key allies on cybersecurity policy and operational cooperation. Leveraging pre-existing relationships among Computer Security Incident Response Teams (CSIRTs), DHS has established a preliminary framework for cooperation on cybersecurity policy, watch and warning, and incident response with several other nations. DHS is also participating in the establishment of an International Watch and Warning Network (IWWN) among cybersecurity policy, computer emergency response, and law enforcement participants from 15 countries. The IWWN will provide a mechanism by which the participating countries can share information to build global cyber situational awareness and coordinate incident response.
- **Partnerships to Address Cyber Aspects of CIKR Protection**: The Federal Government leverages existing agreements such as the SPP and the JCG with the United Kingdom to address the Information Technology Sector and cross-cutting cybersecurity as part of CIKR protection. The trilateral SPP builds on existing bilateral agreements between the United States and Canada and the United States and Mexico by providing a forum to address issues on a dual binational basis. In the context of the JCG, DHS established an action plan to address cybersecurity, watch, warning, incident response, and other strategic initiatives.

4.2 Information Sharing: A Network Approach

The effective implementation of the NIPP is predicated on active participation by government and private sector partners in meaningful, multidirectional information sharing. When owners and operators are provided with a comprehensive picture of threats or hazards to CIKR and participate in ongoing multidirectional information flow, their ability to assess risks, make prudent security investments, and develop appropriate resiliency strategies is substantially enhanced. Similarly, when the government is provided with an understanding of private sector information needs, it can adjust its information collection, analysis, synthesis, and dissemination activities accordingly.

The NIPP information-sharing approach constitutes a shift from a strictly hierarchical to a networked model, allowing distribution and access to information both vertically and horizontally, as well as the ability to enable decentralized decisionmaking and actions. The objectives of the network approach are to:

- Enable secure multidirectional information sharing between and across government and industry that focuses, streamlines, and reduces redundant reporting to the greatest extent possible;
- Implement a common set of all-hazards communications, coordination, and information-sharing capabilities for all CIKR partners;
- Provide CIKR partners with a robust communications framework tailored to their specific information-sharing requirements, risk landscape, and protective architecture;
- Provide CIKR partners with a comprehensive common operating picture that includes timely and accurate information about natural hazards, general and specific terrorist threats, incidents and events, impact assessments, and best practices;
- Provide CIKR partners with timely incident reporting and verification of related facts that owners and operators can use with confidence when considering how evolving incidents might affect their risk posture;
- Provide a means for State, local, tribal, territorial, and private sector partners to be integrated, as appropriate, into the intelligence cycle, to include providing input to the development of intelligence requirements;
- Enable the multidirectional flow of information required for CIKR partners to assess risks, conduct risk management activities, invest in security measures, and allocate resources; and
- Protect the integrity and confidentiality of sensitive information.

Within the CIKR community, information sharing is a means to an end. The objective of an effective environment for information sharing is to provide timely and relevant information that partners can use to make decisions and take the necessary actions to manage CIKR risk.

The CIKR Information-Sharing Environment (ISE) supports three levels of decisionmaking and action: (1) strategic planning and investment, (2) situational awareness and preparedness, and (3) operational planning and response. It provides policy, governance, planning, and coordination of information sharing, as well as a forum for identifying the types of information necessary for partners to make appropriate decisions and take the necessary actions for effective risk management.

Figure 4.2 illustrates the broad concept of the NIPP multidirectional, networked information-sharing approach within the CIKR ISE. This network consists of components that are connected by a national communications platform, the Homeland Security Information Network (HSIN). HSIN is an all-hazards communications system developed by State and local authorities that connects: all 50 States; 5 territories; Washington, DC; and 50 major urban areas. HSIN is one of the key DHS technology tools for strengthening the protection and ensuring the reliable performance of the Nation's critical infrastructure through communication, coordination, and information sharing. It is an Internet-based platform that enables secure, encrypted, unclassified, and for official use only (FOUO) communication between DHS and vetted members within and across CIKR sectors so that partners can obtain, analyze, and share information. The diagram illustrates how this information exchange capability is used for two-way and multidirectional information sharing among: DHS; the Federal Intelligence Community; Federal departments and agencies; State, local, and tribal jurisdictions; and the private sector. The connectivity of the network also allows these partners to share information and coordinate among themselves (e.g., State-to-State coordination). CIKR partners are grouped into nodes in the information-sharing network approach.

4.2.1 Supporting the CIKR Protection Mission

The primary objectives of the NIPP networked approach to information sharing include enhancing situational awareness and maximizing the ability of government and private sector partners at all levels to assess risks and execute risk-mitigation programs and activities. Implementation of the Nation's CIKR protection mission depends on the ability of the government to receive and provide timely, actionable information on emerging threats to CIKR owners and operators and security professionals to support the necessary steps to mitigate risk.

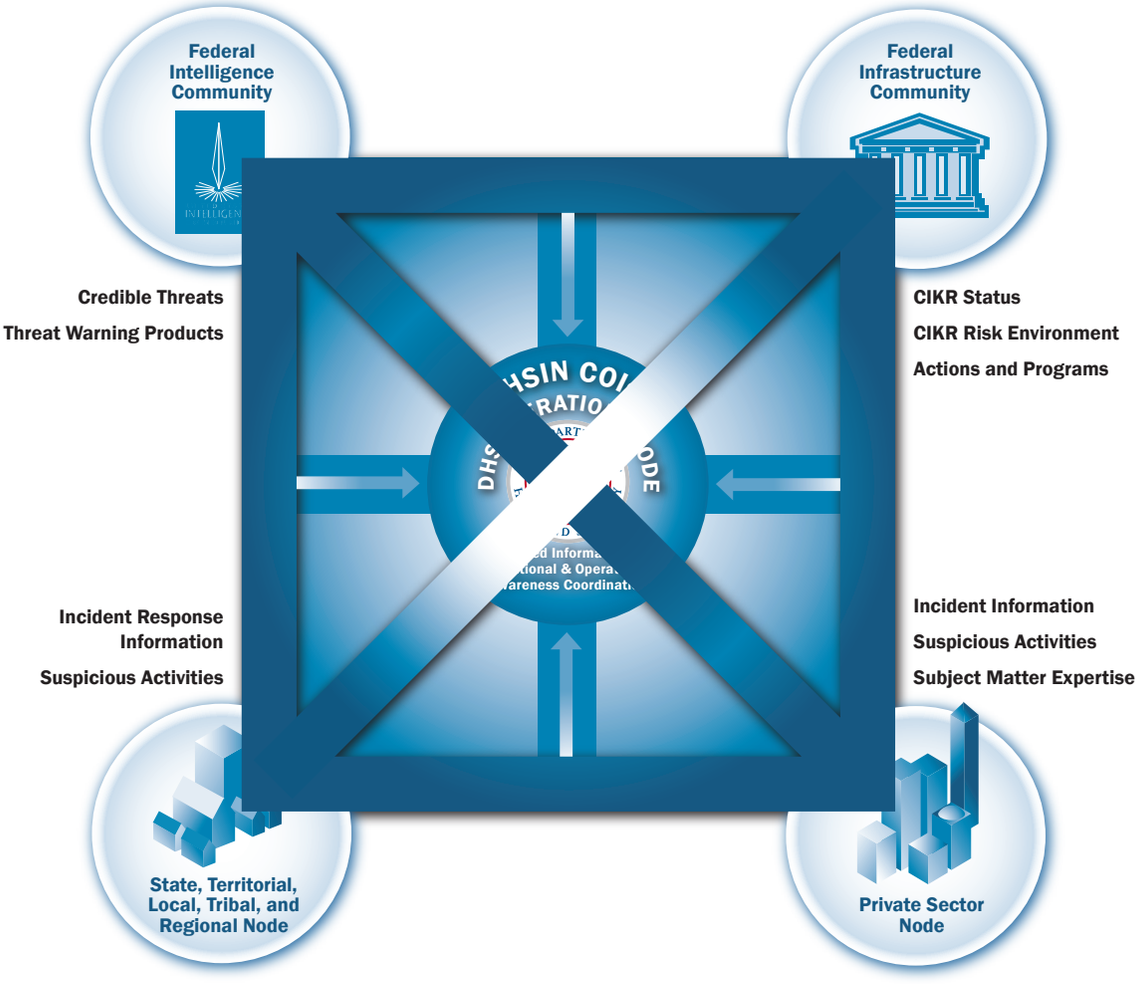
Ongoing and future information-sharing initiatives generally fall within one of four overarching categories:

- **Planning**: All partners have a stake in setting the individual information requirements that best suit the needs of each CIKR sector, driven by the activities in which they need to participate to mitigate CIKR risk. DHS, in conjunction with: the SSAs; SCCs; and other State, local, tribal, territorial, and private sector partners, will collaboratively develop and disseminate an Annual CIKR Protection Information

Requirements Report that summarizes the States and the sectors' input and makes recommendations for information requirements. The Information Requirements Report will be included in the National CIKR Protection Annual Report. In addition to this process, DHS will coordinate with the Intelligence Community to support information collection that reflects the emerging requirements provided by the SSAs and State, local, tribal, territorial, and private sector partners.

- **Information Collection**: Private sector participation in information collection generally is voluntary in nature and includes providing subject matter expertise and operational, vulnerability, and consequence data. Private sector partners also report suspicious activity that could signal pre-operational terrorist activity to the DHS National Operations Center (NOC) through the National Infrastructure Coordinating Center (NICC). Information shared by the private sector, including that which is protected by PCII or other approaches, is integrated into government-collected information to produce comprehensive threat assessments and threat warning products.
- **Analysis**: HITRAC is responsible for integrating CIKR-specific vulnerability and consequence data with threat information to produce actionable risk assessments used to inform CIKR risk-mitigation activities at all levels. HITRAC analysts work closely with CIKR sector subject matter experts and fusion centers to ensure that these products address the individual requirements of each sector and help actuate corresponding security activities.
- **Dissemination and Decisionmaking**: DHS assessments, such as Site Assistance Visits (SAVs) and Buffer Zone Protection Plans (BZPs), which may include information afforded PCII protection, are shared across the sectors through electronic dissemination, posting to HSIN portals, and direct outreach by DHS. During natural disasters, NISAC provides detailed analyses of the impact of disruptions to CIKR. For

Figure 4-2: NIPP Networked Information-Sharing Approach



example, annually before each hurricane season, NISAC posts to HSIN detailed analyses of impacts to CIKR for areas where hurricane landfall is most likely. Similarly, posted on HSIN are operational cross-sector and sector-specific daily and monthly reports that are culled from open sources. Alerts and notifications of vulnerabilities and incidents are sent to the CIKR sectors and their partners in Federal, State, and local agencies as the necessity arises. These efforts and others provide the private sector with timely, actionable information to enhance situational awareness and enable all-hazards planning activities.

4.2.1.1 Balancing the Sharing and Protection of Information

Effective information sharing relies on the balance between making information available and the ability to protect information that may be sensitive, proprietary, or the disclosure of which might compromise ongoing law enforcement, intelligence, or military operations or methods.

Distribution of information is based on using appropriate protocols for information protection. Whether the sharing is top-down (by partners working with national-level information such as system-wide aggregate data or the results of emergent threat analysis from the Intelligence Community) or bottom-up (by field officers or facility operators sharing detailed and location-specific information), the network approach places shared responsibility on all CIKR partners to maintain appropriate and protected information-sharing practices.

4.2.1.2 Top-Down and Bottom-Up Sharing

During incident situations, DHS monitors risk management activities and CIKR status at the functional/operations level, the local law enforcement level, and the cross-sector level. Information sharing may also incorporate information that comes from pre- and post-event natural disaster warnings and reports. While information sharing is multidirectional within the networked model, there are two primary approaches to information sharing during or in response to a threat or incident.

- **Top-Down Sharing**: Under this approach, information regarding a potential terrorist threat originates at the national level through domestic and/or overseas collection and fused analysis, and is subsequently routed to State and local governments, CIKR owners and operators, and other Federal agencies for immediate attention and/or action. This type of information is generally assessed against DHS analysis reports and integrated with CIKR-related information and data from a variety of government and private sector sources. The result of this integration is the development of timely information products, often produced within hours, that are available for appropriate dissemination to CIKR partners based on previously specified reporting processes and data formats.
- **Bottom-Up Sharing**: State, local, tribal, private sector, and nongovernmental organizations report a variety of security- and incident-related information from the field using established communications and reporting channels. This bottom-up information is assessed by DHS and its partners in the intelligence and law enforcement communities in the context of threat, vulnerability, consequence, and other information to illustrate a comprehensive risk landscape.

On January 18, 2007, the National Program Manager of the Information Sharing Environment (PM-ISE) and the Federal Information Sharing Council, both established by the Intelligence Reform and Terrorism Prevention Act of 2004, incorporated the CIKR ISE into the national ISE framework. The PM-ISE is seated in the Office of the Director of National Intelligence. Both the National Information Sharing Strategy issued in October 2007 and the Information Sharing Environment Implementation Plan issued in November 2006 recognized that private sector participation in the ISE is composed primarily of CIKR owners and operators, and recognized the role of the NIPP in defining and establishing this portion of the ISE. The PM-ISE designated IP as the Federal Lead for the implementation of the CIKR ISE within the national ISE.

Threat information that is received from local law enforcement or private sector suspicious activity reporting is routed to DHS through the NICC and the NOC. The information is then routed to intelligence and operations personnel to support further analysis or action as required. In the context of evolving threats or incidents, further national-level analyses may result in the development and dissemination of a variety of HITRAC products as discussed in chapter 3. Further information-sharing and incident management activities are based on the results of the integrated national analysis and the needs of key decisionmakers.

DHS also monitors operational information such as changes in local risk management measures, pre- and post-incident disaster or emergency response information, and local law enforcement activities. Monitoring local incidents contributes to a comprehensive picture that supports incident-related damage assessment, recovery prioritization, and other national- or regional-level planning or resource allocation efforts. Written products and reports that result from the

ongoing monitoring are shared with relevant CIKR partners according to appropriate information protection protocols.

4.2.2 The CIKR Information-Sharing Environment

As specified in the Intelligence Reform and Terrorism Prevention Act of 2004, the Federal Government is working with State and local partners and the private sector to create the ISE for terrorism and homeland security information, in which access to such information is matched to the roles, responsibilities, and missions of all organizations engaged in countering terrorism and is timely and relevant to their needs. It is important to note that most of the information shared daily with the CIKR ISE is necessary for coordination and management of risks resulting from natural hazards and accidents. Consequently, for information sharing to be efficient and sustainable for CIKR owners and operators, the same environment needs to be used to share terrorism information.

With its breadth of participants and the complexity of the CIKR protection mission served, CIKR information sharing breaks new ground. It also creates business risks for the owners and operators. Significant questions are raised, such as: What information is required for a productive two-way exchange? How is information most efficiently delivered and to whom to elicit effective action? How is information—both proprietary and government—appropriately protected? How will the sectors take appropriate action in coordination with all levels of government? How can business risks be mitigated when an exchange takes place?

Of particular criticality is the coordination of CIKR information sharing at the national level with that at the local level, where most decisions are made and actions are taken to support the CIKR protection mission. The integration of the CIKR ISE into the national ISE as its private sector component, in recognition of its comprehensiveness and engagement between CIKR owners and operators and all levels of government, strengthens the foundation for effective coordination.

4.2.2.1 CIKR ISE Coordination and Governance

A necessary component for implementing the CIKR ISE is the sector partnership model, which provides the framework for developing requirements for process, policy, technology, levels of performance, and content. It also provides the essential characteristics for defining the "trusted" environment. By using the sector partnership model to develop requirements, the CIKR ISE accommodates a broad range of sector cultures, operations, and risk management approaches and recognizes the unique policy and legal challenges for full two-way sharing of information between the CIKR owners and operators and the various levels of government.

4.2.2.2 Primary Information-Sharing Support Mechanisms

The CIKR ISE encompasses a number of mechanisms that facilitate the flow of information, mitigate obstacles to voluntary information sharing by CIKR owners and operators, and provide feedback and continuous improvement for NIPP information-sharing structures and processes. Other supporting technologies and more traditional methods of communications will continue to support CIKR protection, as appropriate, and will be fully integrated into the network approach.

The Sector Information-Sharing Maturity Model

This capability provides a DHS-supported process to the Sector and Government Coordinating Councils to identify, document, develop, and implement, when needed, core sector-specific and cross-sector coordination and communication business processes among CIKR owners and operators and their government counterparts at all levels. The five core processes for each sector include: alerts, warnings, and notifications; suspicious activity reporting; data management; incident response communication; and routine steady-state collaboration and communication. Defining these business processes in the form of standard operating procedures identifies the necessary participants, clarifies roles and responsibilities, and pre-establishes the necessary and appropriate related actions to be taken by sector and government participants. This capability includes support for the annual testing of these business processes by the sectors to ensure their continued validity and usefulness to their stakeholders.

HSIN

When fully deployed, the HSIN will constitute a robust and significant information-sharing system that supports NIPP-related steady-state CIKR protection and NRF-related incident management activities, as well as serving the information-sharing processes that form the bridge between these two homeland security missions. The linkage between these sets of activities results in a dynamic view of the strategic risk and evolving incident landscape. HSIN functions as one of a number of mechanisms that enable DHS, the SSAs, and other partners to share information. When HSIN is fully developed, users will be able to access ISE terrorism information based on their roles, responsibilities, and missions. The HSIN is composed of multiple, non-hierarchical communities of interest (COIs) that offer CIKR partners the means to share information based on secure access. COIs provide virtual areas where groups of participants with common concerns, such as law enforcement, counterterrorism, critical infrastructure, emergency management, intelligence, international, and other topics, can share information. This structure allows government

and industry partners to engage in collaborative exchanges, based on specific sector-generated information requirements, mission emphasis, or interest level. Within the HSIN-Critical Sectors COI, each sector establishes the rules for participation, including the vetting and verification processes that are appropriate for the sector CIKR landscape and the requirements for information protection. For example, in some sectors, applicants are vetted through the SCC or the ISAC; others may require participants to be documented members of a specific profession, such as law enforcement.

DHS and the SSAs work with other partners to measure the efficacy of the network and to identify areas in which new mechanisms or supporting technologies are needed. The HSIN and the key nodes of the NIPP information-sharing approach are detailed in the following sections. By offering a user-friendly, efficient conduit for information sharing, HSIN enhances the combined effectiveness in an all-hazards environment. HSIN network architecture design is informed by experience gained by DoD and other Federal agencies in developing networks to support similar missions. It supports a secure common operating picture (COP) for all command or watch centers, including those of supporting emergency management and public health activities.

4.2.2.3 Facilitating Usefulness of Information: iCAV and DHS Earth

An important resource that DHS uses to facilitate networked-based information sharing is the iCAV suite of tools and the underlying Geospatial Information Infrastructure (GII). The iCAV and DHS Earth viewers, as well as the GII, provide mechanisms for: industry; Federal, State, and local governments; and other partners to exchange static and real-time information supporting situational and strategic awareness using standards-based information exchange mechanisms. While the iCAV suite of tools permits the viewing of this information in a dynamic map, the GII and IDW provide additional capabilities that allow the data to be shared, stored, and archived in secure, federally compliant standard formats. The iCAV suite of tools also provides the ability to integrate or link a variety of systems and numerous users, ranging from local first-responders to interested agencies within the Federal Government. Through iCAV and DHS Earth, DHS connects previously stove-piped systems, providing consistent, mission-specific COPs across organizational boundaries, fostering horizontal and vertical CIKR information sharing with mission partners.

4.2.3 Federal Intelligence Node

The Federal Intelligence Node, which comprises national Intelligence Community agencies, SSA intelligence offices, and the DHS Office of Intelligence and Analysis (OI&A), identifies and establishes the credibility of general and specific threats. This node also includes national, regional, and field-level information-sharing and intelligence center entities that contribute to information sharing in the context of the CIKR protection mission.

At the national level, these centers include, but are not limited to, the HITRAC, the FBI-led National Joint Terrorism Task Force (NJTTF), the National Counterterrorism Center (NCTC), and the National Maritime Intelligence Center.

- HITRAC analyzes and integrates threat information and works closely with components of the other NIPP information-sharing nodes to generate and disseminate threat warning products and risk analyses to CIKR partners, both internal and external to the network, as appropriate.
- The NJTTF mission is to enhance communications, coordination, and cooperation among Federal, State, local, and tribal agencies representing the intelligence, law enforcement, defense, diplomatic, public safety, and homeland security communities by providing a point of fusion for terrorism intelligence and by supporting Joint Terrorism Task Forces (JTTFs) throughout the United States.
- The NCTC serves as the primary Federal organization for analyzing and integrating all intelligence possessed or acquired by the U.S. Government that pertains to terrorism and counterterrorism, except purely domestic counterterrorism information. The NCTC may, as consistent with applicable law, receive, retain, and disseminate information from any Federal, State, or local government or other source necessary to fulfill its responsibilities.
- The U.S Coast Guard Intelligence Coordination Center, collocated with the Office of Naval Intelligence at the National Maritime Intelligence Center, serves as the central point of connectivity to fuse, analyze, and disseminate information and intelligence related to the Maritime Transportation System.

At the regional and field levels, Federal information-sharing and intelligence centers include entities such as the local JTTFs, the DHS/DOJ-sponsored Project Seahawk, and FBI Field Intelligence Groups that provide the centralized intelligence/information-sharing component in every FBI field office.

4.2.4 Federal Infrastructure Node

The Federal Infrastructure Node, which comprises DHS, SSAs, GCCs, and other Federal departments and agencies, gathers and receives threat, incident, and other operational information from a variety of sources (including a wide range of watch/operations centers). This information enables assessment of the status of CIKR and facilitates the development and dissemination of appropriate real-time threat and warning products and corresponding protective measures recommendations to CIKR partners (see chapter 3). Participants in the Federal node collaborate with CIKR owners and operators to gain input during the development of threat and warning products and corresponding protective measures recommendations.

4.2.5 State, Local, Tribal, Territorial, and Regional Node

This node provides links among: DHS; the SSAs; and partners at the State, local, tribal, territorial, and regional levels. Several established communications channels provide protocols for passing information from the local to the State to the Federal level and disseminating information from the Federal Government to other partners. The NIPP network approach augments these established communications channels by facilitating two-way and multidirectional information sharing. Members of this node provide incident response, first-responder information, and reports of suspicious activity to the FBI and DHS for the purposes of awareness and analysis. Homeland security advisors receive and further disseminate coordinated DHS/FBI threat and warning products, as appropriate.

Numerous States and urban area jurisdictions also have established fusion centers or terrorism early warning centers to facilitate a collaborative process among law enforcement, public safety, other first-responders, and private entities to collect, integrate, evaluate, analyze, and disseminate criminal intelligence and other information that relates to CIKR protection.

4.2.5.1 State and Local Fusion Centers

Another key mechanism for information exchange at the local level is the SLFCs. SLFCs are developing or integrating operational capabilities that focus on securing CIKR and advancing Federal, State, local, and private sector CIKR protection efforts. These capabilities should incorporate the dissemination of tailored, timely, and actionable analytical products related to CIKR to maximize information sharing and support the risk-reduction activities of the CIKR protection partners. Through such efforts, the capability should be able to support a comprehensive understanding of the threat, local CIKR vulnerabilities, the potential consequences of attacks, and the effects of risk-mitigation actions not only on risk reduction, but also on business operations within the private sector.

The CIKR functionality described above should be integrated with all other SLFC capabilities to assist fusion centers in achieving their mission. This CIKR functionality should correlate with and complement the baseline capabilities developed for SLFCs. Guidance for SLFCs that support CIKR protection activities is being developed as an appendix to the *Baseline Capabilities for State and Major Urban Area Fusion Centers*. (This document may be obtained at www.it.ojp.gov.) This guidance identifies the additional capabilities that SLFCs should achieve to effectively integrate CIKR protection activities into their analytic and information/intelligence-sharing processes and describes how SLFCs can support risk-reduction efforts taken by Federal, State, local, and private sector partners.

4.2.6 Private Sector Node

The Private Sector Node includes CIKR owners and operators, SCCs, ISACs, and trade associations that provide incident information, as well as reports of suspicious activity that may indicate actual or potential criminal intent or terrorist activity. DHS, in return, provides all-hazards warning products, recommended protective measures, and alert notification to a variety of industry coordination and information-sharing mechanisms, as well as directly to affected CIKR owners and operators.

The NIPP network approach connects and augments existing information-sharing mechanisms, where appropriate, to reach the widest possible population of CIKR owners and operators and other partners. Owners and operators need accurate and timely incident and threat-related information in order to effectively: manage risk; enable post-event response and recovery; and make decisions regarding protection strategies, partnerships, mitigation plans, security measures, and investments for addressing risk.

Information exchange between fusion centers and local partners:

- **Site-specific risk information;**
- **Interdependency information;**
- **Suspicious activity reports;**
- **Communications capability information;**
- **Adversary tactics, techniques, and procedures;**
- **Best practices;**
- **Standard operating procedures for incident response; and**
- **Emergency contact/alert information.**

HSPD-7 and the NIPP recognize that CIKR sectors have diverse approaches to establishing their own sectors' information-sharing programs that will most effectively and efficiently meet the requirements of their industry structures, operating cultures, and regulatory regimes. Each sector has the ability to implement a tailored information-sharing solution that may include: privately owned and operated ISACs; voluntary standards development organizations; or other 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.

ISACs provide an example of a private sector information-sharing and analysis mechanism. Originally recommended by Presidential Decision Directive 63 (PDD-63) in 1998, ISACs are private sector-specific entities that advance physical and cyber CIKR protection by establishing and maintaining collaborative frameworks for operational interaction between and among members and external partners. ISACs, as identified by the sector's SCC, typically serve as the tactical and operational arms for 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 the appropriate governmental agencies; identifying and disseminating knowledge and best practices; and promoting education and awareness.

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. Most ISACs are members of the ISAC Council, which provides the mechanism for cross-sector sharing of operational information. Sectors that do not have ISACs per se use other mechanisms that participate in the HSIN and other CIKR protection information-sharing arrangements.

4.2.7 DHS Operations Node

The DHS Operations Node maintains close working relationships with other government and private sector partners to enable and coordinate an integrated operational picture, provide operational and situational awareness, and facilitate CIKR information sharing within and across sectors. DHS and other Federal watch/operations centers provide, on a 24/7 basis, the capability required to enable the real-time alerts and warnings, incident reporting, situational awareness, and assessments needed to support CIKR protection.

The principal purpose of a watch/operations center is to collect and share information. Therefore, the value and effectiveness of such centers is largely dependent on a timely, accurate, and extensive population of information sources. The NIPP information-sharing network approach virtually integrates numerous primary watch/operations centers at various levels to enhance information exchange, providing a far-reaching network of awareness and coordination.

4.2.7.1 National Operations Center[8]

The NOC serves as the Nation's hub for domestic incident management operational coordination and situational awareness. The NOC is a standing interagency organization that operates on a 24/7 basis, fusing law enforcement, national intelligence, emergency response, and private sector reporting. The NOC facilitates homeland security information-sharing and operational coordination among Federal, State, local, tribal, and private sector partners, as well as select members of the international community. As such, it is at the center of the NIPP information-sharing network.

The NOC information-sharing and coordination functions include:

- **Information Collection and Analysis**: The NOC maintains national-level situational awareness and provides a centralized, real-time flow of information. An NOC common operating picture is generated using data collected from across the country to provide a broad view of the Nation's current overall risk and preparedness status. Using the common operating picture, NOC personnel, in coordination with the FBI and other agencies, as appropriate, perform initial assessments to gauge the terrorism nexus and track actions taking place across the country in response to a threat, natural disaster, or accident. The information compiled by the NOC is distributed to partners, as appropriate, and is accessible to affected CIKR partners through the HSIN.
- **Situational Awareness and Incident Response Coordination**: The NOC provides the all-hazards information needed to help make decisions and define courses of action.
- **Threat Warning Products**: DHS jointly reviews threat information with the FBI, the Intelligence Community, and other Federal departments and agencies on a continuous basis. When a threat is determined to be credible and

[8] The Federal Response to Hurricane Katrina: Lessons Learned, issued by the Homeland Security Council, February 2006, recommended the establishment of the NOC as a single entity to unify situational awareness and response, recovery, and mitigation functions. The NOC replaces the DHS Homeland Security Operations Center.

actionable, DHS is responsible for coordinating with these Federal partners in the development and dissemination of threat warning products. This coordination ensures, to the greatest extent possible, the accuracy and timeliness of the information, as well as concurrence by Federal partners.

DHS disseminates threat warning products to Federal, State, local, and tribal governments, as well as to private sector organizations and international partners as COI members through the HSIN, established email distribution lists, and other methods, as required:

- **Threat Advisories**: Contain actionable threat information and provide recommended protective actions based on the nature of the threat. They also may communicate a national, regional, or sector-specific change in the HSAS threat condition.
- **Homeland Security Assessments**: Communicate threat information that does not meet the timeliness, specificity, or criticality criteria of an advisory, but it is pertinent to the security of U.S. CIKR.

The NOC comprises four sub-elements: the NOC Headquarters Element (NOC-HQE), the National Response Coordination Center (NRCC), the intelligence and analysis element, and the NICC:

- **NOC Headquarters Element**: The NOC-HQE is a multi-agency center that provides overall Federal prevention, protection, and preparedness coordination. The NOC-HQE integrates representatives from DHS and other Federal departments and agencies to support steady-state threat-monitoring requirements and situational awareness, as well as operational incident management planning and coordination. The organizational structure of the NOC-HQE is designed to integrate a full spectrum of interagency subject matter expertise, operational planning capability, and reach-back capability to meet the demands of a wide range of potential incident scenarios.
- **National Response Coordination Center**: The NRCC is a multi-agency team operating from FEMA Headquarters that functions as the operational component of the DHS NOC. The NRCC coordinates personnel and resource deployments to support disaster operations and prioritizes interagency allocation of resources. It also maintains situational awareness linkages with regional, State, and local partners and a 24/7 watch team.
- **Intelligence and Analysis Element**: The intelligence and analysis element is responsible for interagency intelligence collection requirements, analysis, production, and product dissemination for DHS, to include homeland security threat warnings, advisory bulletins, and other information pertinent to national incident management (see section 4.2.4).
- **National Infrastructure Coordinating Center**: The NICC, which operates on a 24/7 basis, is a watch/operations center that maintains ongoing operational and situational awareness of the Nation's CIKR sectors. As a CIKR-focused element of the NOC, the NICC provides a centralized mechanism and process for information sharing and coordination among the government, SCCs, GCCs, ISACs, and other industry partners. The NICC receives situational, operational, and incident information from the CIKR sectors in accordance with the information-sharing protocols established in the NRF. The NICC also disseminates products originated by HITRAC that contain all-hazards warning, threat, risk, and CIKR protection information:
  - *Alerts and Warnings:* The NICC disseminates threat-related and other all-hazards information products to an extensive customer base of private sector partners.
  - *Suspicious Activity and Potential Threat Reporting:* The NICC receives and processes reports from the private sector on suspicious activities or potential threats to the Nation's CIKR. The NICC documents the information provided, compiles additional details surrounding the suspicious activity or potential threat, and forwards the report to DHS sector specialists, the NOC, HITRAC, and the FBI.
  - *Incidents and Events:* When an incident or event occurs, the NICC coordinates with DHS sector specialists, industry partners, and other established information-sharing mechanisms to communicate pertinent information. As needed, the NICC generates reports detailing the incident, as well as the sector impacts (or potential impacts), and disseminates them to the NOC.

During Hurricanes Gustav and Ike in 2008, the NICC facilitated critical incident-related information sharing between the government and CIKR owners and operators. Through the Infrastructure Protection Executive Notification Service (ENS), the NICC provided situation reports to the SSAs, which, in turn, contacted their respective CIKR owners and operators and related government agencies to develop impact assessments. Throughout both hurricanes, the SSAs submitted reports twice daily via a secure Web site. These reports included information on damage assessments, restoration activities, and key issues or concerns. The NICC compiled the SSA reports and uploaded the CIKR portion of the DHS Situation Report into the COP and/or HSIN-CS for access by the SSAs and CIKR owners and operators.

– *National Response Planning and Execution*: The NICC supports the NRF by facilitating information sharing among the SCCs, GCCs, ISACs, and other partners during CIKR mitigation, response, and recovery activities.

4.2.7.2 National Coordinating Center for Telecommunications

Pursuant to Executive Order 12472, the National Communications System (NCS) assists the President, National Security Council, Homeland Security Council, Office of Science and Technology Policy (OSTP), and OMB in the coordination and provision of NS/EP communications for the Federal Government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution. As called for in the Executive Order, the NCS has established the National Coordinating Center for Telecommunications (NCC), which is a joint industry-government entity. Under the Executive Order, the NCC assists the NCS in the initiation, coordination, and recovery of NS/EP communications services or facilities under all conditions of crisis or emergency. The NCC regularly monitors the status of communications systems. It collects situational and operational information on a regular basis, as well as during a crisis, and provides information to the NCS. The NCS, in turn, shares information with the White House and other DHS components.

4.2.7.3 United States Computer Emergency Readiness Team

The United States Computer Emergency Readiness Team (US-CERT), which operates on a 24/7 basis, is a single point of contact for cyberspace analysis, warning, information sharing, and incident response and recovery for CIKR partners. It is a partnership between DHS and the public and private sectors designed to enable protection of cyber infrastructure and to coordinate the prevention of and response to cyber attacks across the Nation.

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

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

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

4.2.8 Other Information-Sharing Nodes

DHS, other Federal agencies, and the law enforcement community provide additional services and programs that share information supporting CIKR protection with a broad range of partners. These include, but are not limited to, the following:

- **Sharing National Security Information**: DHS sponsors security clearances for designated private sector owners and operators to promote the sharing of classified information using currently available methods and systems.
- **FBI Law Enforcement Online (LEO)**: LEO can be accessed by any approved employee of a Federal, State, or local law enforcement agency, or approved member of an authorized law enforcement special interest group. LEO provides a communications mechanism to link all levels of law enforcement throughout the United States.
- **RISSNET™** is a secure nationwide law enforcement and information-sharing network that operates as part of the Regional Information Sharing Systems (RISS) Program. RISS is composed of six regional centers that share intelligence and coordinate efforts targeted against criminal networks, terrorism, cyber crime, and other unlawful activities that cross jurisdictional lines. RISSNET features include online access to a RISS electronic bulletin board, databases, RISS center Web pages, secure email, a RISS search engine, and other center resources. The RISS program is federally funded and administered by the DOJ/Bureau of Justice Assistance.

- **FBI InfraGard**: InfraGard is a partnership among the FBI, other governmental entities, and the private sector. The InfraGard National Membership Alliance is an association of businesses, academic institutions, State and local law enforcement agencies, and other participants that enables the sharing of knowledge, expertise, information, and intelligence related to the protection of U.S. CIKR from physical and cyber threats.
- **The United States Coast Guard (USCG) HOMEPORT**: The HOMEPORT Web site is an Internet-enabled venue capable of supporting the sharing of sensitive information among Federal, State, local, and private sector maritime regulatory or security personnel. HOMEPORT is the primary means of informing members of local Maritime Security Committees.
- **Interagency Cybersecurity Efforts**: The intelligence and law enforcement communities have various information-sharing mechanisms in place. Examples include:
  - *U.S. Secret Service Electronic Crimes Task Forces (ECTFs)*: ECTFs prevent, detect, and investigate electronic crimes, cyber-based attacks, and intrusions against CIKR and electronic payment systems, and provide interagency information sharing on related issues.
  - *Cybercop Portal*: The DHS-sponsored Cybercop portal is a secure Internet-based information-sharing mechanism that connects more than 5,300 members of the law enforcement community, bank investigators, and the network security specialists involved in electronic crimes investigations.

4.3 Protection of Sensitive CIKR Information

NIPP implementation will rely greatly on critical infrastructure information provided by the private sector and State and local governments. Much of this is sensitive business or security information that could cause serious damage to companies, the economy, and public safety or security through unauthorized disclosure or access to this information.

The Federal Government has a statutory responsibility to safeguard information collected from or about CIKR activities. Section 201(d)(12)(a) of the Homeland Security Act requires DHS to "ensure that any material received pursuant to this Act 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 PCII Program, to ensure that CIKR information is properly safeguarded. In addition to the PCII Program, other programs and procedures used to protect sensitive information include Sensitive Security Information for transportation activities, Unclassified Controlled Nuclear Information (UCNI), Safeguards Information, contractual provisions, classified national provisions, Classified National Security Information, Law Enforcement Sensitive Information, Federal Security Information Guidelines, Federal Security Classification Guidelines, and other requirements established by law.

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 institutes a means for the voluntary sharing of private sector, State, and local CIKR information with the Federal Government while providing assurances that the information will be exempt from public disclosure and will be properly safeguarded.

The PCII Program, which operates under the authority of the CII Act and the implementing regulation (6 Code of Federal Regulations (CFR) Part 29 (the Final Rule)), defines both the requirements for submitting CII and those that governmental entities must meet for accessing and safeguarding PCII. DHS remains committed to making PCII an effective tool for robust information sharing between critical infrastructure owners and operators and the government. For more information, contact the PCII Program Office at pcii-info@dhs.gov. Additional PCII Program information may also be found at www.dhs.gov/pcii.

4.3.1.1 PCII Program Office

The PCII Program Office is responsible for managing PCII Program requirements, developing protocols for handling PCII, raising awareness of the need for protected information sharing between different levels of government and the private sector, and ensuring that programs receiving voluntary CII submissions that have been validated as PCII use approved procedures to continuously safeguard submitted information. The Program Office collaborates with governmental organizations and the private sector to develop information-sharing partnerships that promote greater homeland security.

4.3.1.2 Critical Infrastructure Information Protection

The following processes and procedures apply to all CII submissions:

- Individuals or collaborative groups may submit information for protection to either the PCII Program Office or a Federal PCII Program Manager Designee;
- The PCII Program Office validates the information as PCII if it qualifies for protection under the CII Act;

- All PCII is stored in secure data management systems and CIKR partners follow PCII Program safeguarding, handling, dissemination, and storage requirements established in the Final Rule and promulgated by the PCII Program Office;
- Secure methods are used for disseminating PCII, which may only be accessed by authorized PCII users who have taken the PCII Program training (see section 6.2 for PCII training offerings), have homeland security duties, and have a need to know for the specific PCII;
- Authorized users must comply with the safeguarding requirements defined by the PCII Program Office; and
- Any suspected disclosure of PCII will be promptly investigated.

The Final Rule invested the PCII Program Manager with the authority and flexibility to designate certain types of CII as presumptively valid PCII to accelerate the validation process and to facilitate submissions directly to the SSAs and other Federal partners. This is known as a "categorical inclusion." Specifically, categorical inclusions allow:

- The PCII Program Manager to establish categories of information for which PCII status will automatically apply;
- Indirect submissions to DHS through DHS field representatives and other Federal partners; and
- The PCII Program Office to designate DHS field representatives and Federal partners other than DHS to receive CII indirectly on behalf of DHS, but only the PCII Program Manager is authorized to make the decision to validate a submission as PCII.

The Final Rule enables submitters to submit their CII directly to a PCII Program Manager Designee within a given Federal agency. Interested submitters should contact the PCII Program Office at pcii-info@dhs.gov to determine whether a Federal partner has an appropriate PCII categorical inclusion program established. If not, the PCII Program Office will work with the submitter and the relevant Federal partner to establish a program and facilitate the application of PCII protections to the submitter's CIKR information.

4.3.1.3 Uses of PCII

PCII may be shared with accredited governmental entities, including authorized Federal, State, or local government employees or contractors supporting Federal agencies, only for the purposes of securing CIKR and protected systems. PCII will be used for analysis, prevention, response, and recovery of CIKR threatened by terrorism or other hazards.

PCII may be used to generate advisories, alerts, and warnings relevant to the private sector. Communications available to the public, however, will not contain any actual PCII. PCII can be combined with other information, including classified information to support CIKR protection activities, but must be marked accordingly.

The CII Act specifically authorizes disclosure of PCII without the permission of the submitter to:

- Further an investigation or prosecute a criminal act;
- Either House of Congress, to the extent that they address matters within their jurisdiction, or any related committee, subcommittee, or joint committee; and
- The Comptroller General or any authorized representative of the Comptroller General, while performing the duties of the Government Accountability Office.

4.3.1.4 PCII Protections and Authorized Users

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

- Used appropriately for homeland security purposes;
- Accessed only by authorized and properly trained government employees and contractors with homeland security duties who have a need to know and for non-Federal government employees who have signed a Non-Disclosure Agreement;
- Protected from disclosure under the Freedom of Information Act (FOIA) and similar State and local disclosure laws, and from use in civil litigation and regulatory actions; and
- Protected and handled in a secure manner.

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

- 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
- The CII Act sanctions for unauthorized disclosure of PCII apply only to Federal personnel. In order to become accredited, State and local participating entities must demonstrate that they can apply appropriate State and local penalties for improperly handling sensitive information such as PCII.

PCII is actively used by numerous DHS information collection and assessment tools, including the C/ACAMS, BZPs, and SAVs. PCII also partners with many Federal agencies, notably the Department of Health and Human Services (HHS) and DoD. In addition, the PCII Program actively partners with all State, local, and territorial governments interested in accessing PCII.

4.3.2 Other Information Protection Protocols

Information protection protocols may impose requirements for access or other standard processes for safeguarding information. Information need not be validated as PCII to receive security protection and disclosure restrictions. Several categories of information related to CIKR are considered to be sensitive and require protection, but are not classified. The major categories that currently apply to CIKR are discussed below.

4.3.2.1 Sensitive Security Information (SSI)

The Maritime Transportation Security Act, the Aviation Transportation Security Act, and the Homeland Security Act establish protection for Sensitive Security Information (SSI). The Transportation Security Administration (TSA) and the USCG 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 demonstrate 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 protection pertains to government officials, as well as to Transportation Systems Sector owners and operators.

4.3.2.2 Unclassified Controlled Nuclear Information (UCNI)

DoD and DOE 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 public health and safety 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 Safeguards Information (SGI)

Safeguards Information (SGI) is a special category of sensitive unclassified information authorized by Section 147 of the Atomic Energy Act of 1954, as amended. SGI concerns the physical protection of operating power reactors, spent fuel shipments, strategic special nuclear material, or other radioactive material. While SGI is considered sensitive unclassified information, its handling and protection more closely resemble the handling of classified Confidential information than other sensitive unclassified information. The categories of individuals who are permitted access to SGI and the access requirements are listed in 10 CFR 73.21.

4.3.2.4 Freedom of Information Act Exemptions and Exclusions

FOIA was enacted in 1966 and amended and modified by congressional legislation, including the Privacy Act of 1974, the Electronic Freedom of Information Act of 1996, and the OPEN Government Act of 2007. 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 that protect information, such as informants' names. 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, personnel and medical files, information that Congress exempted by another statute, trade secrets or financial information obtained by the government from individuals, information subject to common law privileges, certain law enforcement records, and information exempt on privacy grounds.

4.3.2.5 Classified Information

Under amended Executive Orders 12958 and 12829, 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 (NSI), including information related to defense against transnational terrorism.

Specific characteristics distinguish classified information from other sensitive information. These include:

- Information can only be designated as classified by a duly empowered authority;
- Information classified by one classification authority must be handled by others in accordance with the guidelines issued by the classifying authority;

- Information must be owned by, produced by or for, or under the control of the Federal Government;
- Unauthorized disclosure of the information could reasonably be expected to result in damage to U.S. national security; and
- The information falls into one or more of the categories of information listed below:
  - 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 related to national security, which includes defense against transnational terrorism;
  - Federal Government programs for safeguarding nuclear materials or facilities;
  - Vulnerabilities or capabilities of systems, installations, infrastructure, projects, plans, or protection services related to national security, which includes defense against transnational terrorism; or
  - Weapons of mass destruction.

Many forms of information related to CIKR protection have these characteristics. This information may be determined to be classified information and must be protected accordingly.

4.3.2.6 Physical Security and Cybersecurity Measures

DHS uses strict information security protocols for the access, use, and storage of sensitive information, including that related to CIKR. 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, login restrictions, session tracking, and data labeling. Appendix 3C provides a discussion of these protections as applied to the IDW.

4.3.2.7 Chemical-Terrorism Vulnerability Information

On April 9, 2007, DHS issued the CFATS. Congress authorized these interim final regulations (IFR) under section 550 of the Department of Homeland Security Appropriations Act of 2007, directing the department to identify, assess, and ensure effective security at high-risk chemical facilities. In section 550, Congress also acknowledged DHS's need to both protect and share chemical facility security information with appropriate third parties. Consequently, DHS included provisions in the IFR to create and explain Chemical-Terrorism Vulnerability Information (CVI), a new category of protected information to protect extremely sensitive information that facilities develop for the purposes of complying with the CFATS, which could be exploited by terrorists. At the same time, CVI allows the sharing of relevant information with State and local government officials who have a need to know CVI in order to carry out chemical facility security activities. Before being authorized to access CVI, individuals will have to complete training to ensure that they understand and comply with the various safeguarding and handling requirements for CVI.

More information on CFATS and CVI, including the CVI Procedures Manual, can be found at www.dhs.gov/chemicalsecurity.

4.4 Privacy and Constitutional Freedoms

Mechanisms detailed in the NIPP are designed to obtain a high level of security while protecting the privacy, civil rights, and civil liberties that form an integral part of America's national character. In providing for effective protection programs, the processes outlined in the NIPP respect privacy, freedom of expression, freedom of movement, freedom from unlawful discrimination, and other liberties that define the American way of life. Compliance with the Privacy Act and governmental privacy regulations and procedures is a key factor that is considered when collecting, maintaining, using, and disseminating personally identifiable information. The following DHS offices support the NIPP processes:

- **DHS Privacy Office**: Pursuant to Section 222 the Homeland Security Act, DHS has designated a Chief Privacy Officer to establish privacy policy within the Department and to work with programs and offices to ensure their compliance with all applicable privacy laws and policies. The DHS Privacy Office conducts privacy impact assessments which identify potential privacy risks, details steps programs have taken to mitigate those potential risks, and makes recommendations that programs may implement to further reduce risks to privacy. The DHS Chief Privacy Officer, moreover consults regularly with privacy advocates, industry experts, and the public at large to provide transparency and ensure broad input and consideration of privacy issues, so that DHS achieves solutions that protect privacy while enhancing security.

- **DHS Office for Civil Rights and Civil Liberties**: Pursuant to the Homeland Security Act, the Office for Civil Rights and Civil Liberties provides legal and policy advice to department leadership on civil rights and civil liberties issues to ensure our freedoms are preserved while protecting the homeland. The Office for Civil Rights and Civil Liberties also investigates and resolves complaints from the public concerning civil rights and civil liberties abuses or racial, ethnic, or religious profiling.

5. CIKR Protection as Part of the Homeland Security Mission

This chapter describes the linkages between the NIPP, the SSPs, and other CIKR protection strategies, plans, and initiatives that are most relevant to the overarching national homeland security and CIKR protection missions. It also describes how the unified national CIKR protection effort integrates elements of the homeland security mission, including preparedness and activities to prevent, protect against, respond to, and recover from terrorist attacks, major disasters, and other emergencies. Sector-specific linkages to these other national frameworks are addressed in the SSPs.

5.1 A Coordinated National Approach to the Homeland Security Mission

The NIPP provides the structure needed to coordinate, integrate, and synchronize activities derived from various relevant statutes, national strategies, and Presidential directives to create a unified national approach to implementing the CIKR protection mission. The relevant authorities include those that address the overarching homeland security and CIKR protection missions, as well as those that address a wide range of sector-specific CIKR protection-related functions, programs, and responsibilities. This section describes how overarching homeland security legislation, strategies, HSPDs, and related initiatives work together (see figure 5-1). Information regarding sector-specific CIKR-related authorities is addressed in the respective SSPs.

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 CIKR protection efforts and activities. A number of other statutes (as described in chapter 2 and appendix 2A) provide authorities for cross-sector and sector-specific CIKR protection activities. Individual SSPs address relevant sector-specific authorities.

Public Law 110-53, Implementing Recommendations of the 9/11 Commission Act of 2007, further refines and enumerates the authorities specified in the Homeland Security Act and formally assigns key infrastructure protection responsibilities to DHS, including the creation of a database of all national infrastructure to support cross-sector risk assessment and management.

5.1.2 Strategies

The National Strategy 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 strategic direction for the CIKR protection elements of the homeland security mission (see figure 5-1, column 1). A number of other Presidential strategies, such as the National Intelligence Strategy, provide direction and guidance related to CIKR protection on a national or sector-specific basis (see appendix 2A).

5.1.2.1 The National Strategy for Homeland Security

The President's National Strategy for Homeland Security (2002) established protection of America's CIKR 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."

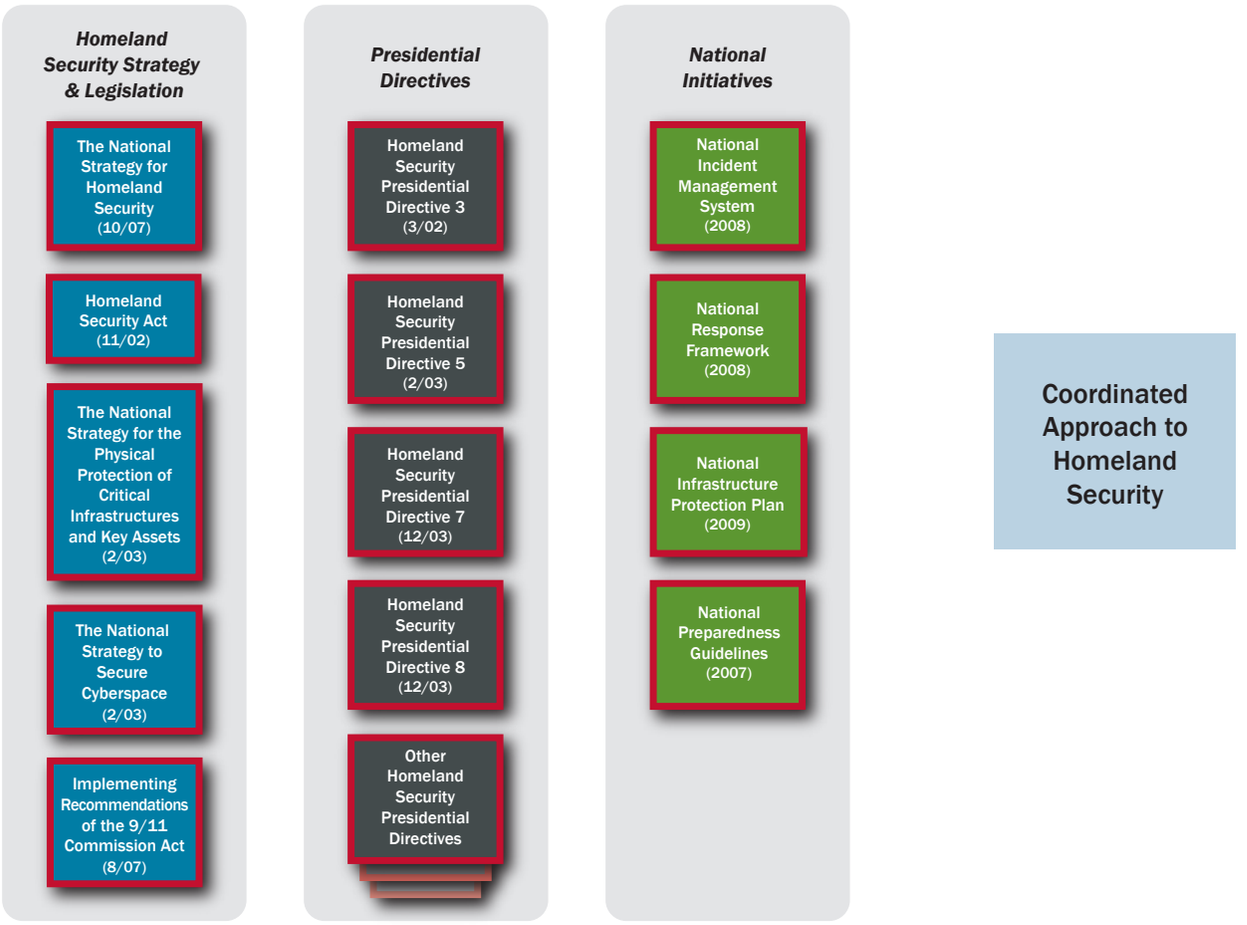
This strategy called for the development of "interconnected and complementary homeland security systems that are reinforcing rather than duplicative, and that ensure essential requirements are met … [and] provide a framework to align the resources of the Federal budget directly to the task of securing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

The 2007 National Strategy for Homeland Security builds on the first National Strategy for Homeland Security and complements both the National Security Strategy issued in March 2006 and the National Strategy for Combating Terrorism issued in September 2006. It reflects the increased understanding of threats confronting the United States, incorporates lessons learned from exercises and real-world catastrophes, and addresses ways to ensure long-term success by strengthening the homeland security foundation that has been built.

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;

Figure 5-1: National Framework for Homeland Security



identifies key initiatives needed to secure each of the CIKR 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 sets forth objectives and specific actions needed to prevent cyber attacks against America's CIKR, identifies and appropriately responds to those responsible for cyber attacks, reduces nationally identified vulnerabilities, and minimizes 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, awareness and training programs, efforts to secure government cyberspace, and international cooperation.

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.

5.1.2.4 Implementing Recommendations of the 9/11 Commission Act of 2007

This act requires the implementation of some of the recommendations made by the 9/11 Commission, to include requiring the Secretary of Homeland Security to: (1) establish department-wide procedures to receive and analyze intelligence from State, local, and tribal governments and the private sector; and (2) establish a system that screens 100 percent of maritime and passenger cargo. The act also established grants to support high-risk urban areas and State, local, and tribal governments in preventing, preparing for, protecting against, and responding to acts of terrorism, and to assist States in carrying out initiatives to improve international emergency communications.

Title IX of the act requires DHS to establish a common set of criteria for private sector preparedness in disaster management, emergency management, and business continuity. These Voluntary Private Sector Preparedness Standards will be accredited and certified by the American National Standards Institute (ANSI) and the American Society for Quality (ASQ) National Accreditation Board (ANAB).

The act also established grants to support high-risk urban areas and State, local, and tribal governments in preventing, preparing for, protecting against, and responding to acts of terrorism.

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 2). 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 incidents that do occur." A number of these are relevant to CIKR protection. 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 CIKR 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.

This section addresses the Homeland Security Presidential Directives that are most relevant to the overarching CIKR protection component of the homeland security mission (e.g., HSPD-3, -5, -7, and -8). Other related Presidential directives, such as: HSPD-9, Defense of the United States Agriculture and Food; HSPD-10, Biodefense for the 21st Century; and HSPD-22, Domestic Chemical Defense, are relevant to CIKR protection in specific sectors and are addressed in further detail in the appropriate SSPs. Additional HSPDs are also described in appendix 2A.

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 also serve as guideposts for the implementation of tailored protective measures by State, local, tribal, and private sector 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 NIMS and the NRF (see figure 5-1, column 4).

The NIMS (December 2008) provides a nationwide template enabling: Federal, State, local, and tribal governments; the private sector; and nongovernmental organizations to work together effectively and efficiently to prevent, protect against, respond to, and recover from incidents regardless of cause, size, and complexity. The NIMS provides a uniform doctrine for command and management, including: Incident Command, Multi-Agency Coordination, and Joint Information Systems; resource, communications, and information management; and application of supporting technologies.

The NRP (December 2004) was superseded by the National Response Framework (January 2008). Both the NRP and the NRF were built on the NIMS template to establish a single, comprehensive framework for the management of domestic incidents (including threats) that require DHS coordination and effective response and engaged partnership by an appropriate combination of: Federal, State, local, and tribal governments; the private sector; and nongovernmental organizations. The NRF includes a CIKR Support Annex that provides the policies and protocols for integrating the CIKR protection mission as an essential element of domestic incident management and establishes the Infrastructure Liaison function to serve as a focal point for CIKR coordination at the field level.

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 CIKR." It mandated development of the NIPP as the primary vehicle for implementing the CIKR 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 CIKR;
- A summary of activities to be undertaken to prioritize, reduce the vulnerability of, and coordinate protection of CIKR;
- 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 NRF and guidance provided in the National Preparedness Guidelines.

HSPD-7 also directed the Secretary of Homeland Security to maintain an organization to serve as a focal point for the security of cyberspace. The NIPP is supported by a series of SSPs, developed by the SSAs in coordination with their public and private sector partners, which detail the approach to CIKR protection goals, initiatives, processes, and requirements for each sector.

5.1.3.4 HSPD-8, National Preparedness

HSPD-8 (December 2003) mandates the development of a national preparedness goal, which was finalized in the National Preparedness Guidelines (see figure 5-1, column 3), 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 "to minimize the impact on lives, property, and the economy."

To do this, the National Preparedness Guidelines provide readiness targets, priorities, standards for assessments and strategies, and a system for assessing the Nation's overall level of preparedness across four mission areas: prevention, protection, response, and recovery. There are four critical elements of the National Preparedness Guidelines:

- **The National Preparedness Vision**, which provides a concise statement of the core preparedness goal for the Nation.
- **The National Planning Scenarios**, which depict a diverse set of high-consequence threat scenarios of both potential terrorist attacks and natural disasters. Collectively, the 15 scenarios are designed to focus contingency planning for homeland security preparedness work at all levels of government and with the private sector. The scenarios form the basis for coordinated Federal planning, training, exercises, and grant investments needed to prepare for emergencies of all types.
- **The Universal Task List (UTL)**, which is a menu of some 1,600 unique tasks that can facilitate efforts to prevent, protect against, respond to, and recover from the major events that are represented by the National Planning Scenarios. It presents a common vocabulary and identifies key tasks that support the development of essential capabilities among organizations at all levels. No entity is expected to perform every task.
- **The Target Capabilities List (TCL)**, which defines 37 specific capabilities that communities, the private sector, and all levels of government should collectively possess in order to respond effectively to disasters.

The National Preparedness Guidelines use capabilities-based planning processes and enable Federal, State, local, and

tribal entities to prioritize needs, update strategies, allocate resources, and deliver programs. The guidelines reference standard planning tools that are applicable to the implementation of the NIPP, including the UTL and the TCL. Like the NIPP, the UTL and TCL are living documents that will be enhanced and refined over time.

Annex 1 (December 2007) to HSPD-8 established a standard and comprehensive approach to national planning intended to enhance the preparedness of the Nation. The annex articulated the U.S. Government policy "to integrate effective policy and operational objectives to prevent, protect against, respond to, and recover from all hazards, and comprises: (a) a standardized Federal planning process; (b) national planning doctrine; (c) resourced operational and tactical capabilities at each Federal department and agency with a role in homeland security; (d) strategic guidance, strategic plans, concepts of operations, and operations plans and, as appropriate, tactical plans; and (e) a system for integrating plans among all levels of government."

5.1.3.5 HSPD-19, Combating Terrorist Use of Explosives in the United States

In February 2007, the President signed HSPD-19, Combating Terrorist Use of Explosives in the United States, requiring the Attorney General to develop a report for the President, including a national strategy and recommendations, on how to more effectively deter, prevent, detect, protect against, and respond to explosive attacks, including the coordination of Federal Government efforts with State, local, tribal, and territorial governments, first-responders, and private sector organizations. HSPD-19 required that the "Attorney General, in coordination with the Secretaries of Defense and Homeland Security and the heads of other Sector-Specific Agencies (as defined in HSPD-7) and agencies that conduct explosive attack detection, prevention, protection, or response activities …develop an implementation plan." HSPD-19 required that the plan implement its policy and any approved recommendations in the report and "include measures to (a) coordinate the efforts of Federal, State, local, territorial, and tribal government entities to develop related capabilities, (b) allocate Federal grant funds effectively, (c) resourced operational and tactical capabilities at each Federal department and agency with a role in homeland security; (d) coordinate training and exercise activities, and (e) incorporate, and strengthen as appropriate, existing plans and procedures to communicate accurate, coordinated, and timely information regarding a potential or actual explosive attack to the public, the media, and the private sector."

The HSPD-19 report presents a holistic approach for improving the Nation's ability to deter, prevent, detect, protect against, and respond to the threat of terrorist explosive and IED attacks on the homeland. The report provides 35 recommendations to enhance and align our current counter-IED capabilities and concludes that in order to improve our national CIKR protection posture, there must be a systematic approach in which all deterrence, prevention, detection, protection, and response efforts are unified. The strategy and recommendations provide a way forward that streamlines and enhances current activities, reducing conflict, confusion, and duplication of effort among interagency partners. The Implementation Plan builds on the policies, strategy, and guidance set forth by the President in HSPD-19 and outlined by the Attorney General and interagency partners in the HSPD-19 Report to the President.

The Secretary of Homeland Security designated IP to coordinate the department's activities and represent DHS in the DOJ-led implementation of HSPD-19. IP efforts to enhance and coordinate the Nation's ability to detect, deter, prevent, and respond to IED attacks against critical infrastructure, key resources, and soft targets include: (1) coordinating national and intergovernmental IED security efforts; (2) conducting requirements, capabilities, and gap analyses; and (3) promoting information-sharing and IED security awareness. DHS collaborated with DOJ to develop the Implementation Plan for Combating Terrorist Use of Explosives in the United States.

HSPD-19 also assigns to DHS specific roles and responsibilities for information sharing and counter-IED research, development, testing, and evaluation. HSPD-19 states that the Secretary of Homeland Security, in coordination with the Attorney General, the Director of National Intelligence, and the Secretaries of State and Defense, will establish and maintain secure information-sharing systems to provide law enforcement agencies and other first-responders with access to detailed information that enhances the preparedness of Federal, State, local, tribal, and territorial government personnel to deter, prevent, detect, protect against, and respond to explosive attacks in the United States.

Additionally, HSPD-19 states that the Secretary of Homeland Security, in coordination with the Attorney General, the Secretary of Defense, and the Director of the Office of Science and Technology Policy, is responsible for coordinating Federal Government research, development, testing, and evaluation activities related to the detection and prevention of, protection against, and response to explosive attacks and the development of explosives render-safe tools and technologies.

5.2 The CIKR Protection Component of the Homeland Security Mission

The result of this interrelated set of national authorities, strategies, 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 CIKR as a steady-state component of routine, day-to-day business operations for government and private sector partners.

The NIPP and NRF are complementary plans that span a spectrum of prevention, protection, response, and recovery activities to enable this coordinated approach on a day-to-day basis, as well as 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 greatest return in terms of national risk management. The NRF addresses response and short-term recovery in the context of domestic threat and incident management. The National Preparedness Guidelines support implementation of both the NIPP and the NRF by establishing national priorities and guidance for building the requisite capabilities to support both plans at all levels of government.

Each of the guiding elements includes specific requirements for DHS and other Federal departments and agencies to build engaged partnerships and work in cooperation and collaboration with State, local, tribal, and private sector partners. This cooperation and collaboration between government and private sector owners and operators is specifically applicable to the CIKR protection efforts outlined in the NIPP.

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

5.3 Relationship of the NIPP and SSPs to Other CIKR Plans and Programs

The NIPP and the SSPs outline the overarching elements of the CIKR 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 and approaches associated with each sector.

Homeland security plans and strategies at the State, local, and tribal levels of government address CIKR protection within their respective jurisdictions, as well as mechanisms for coordination with various regional efforts and other external entities. The NIPP also is designed to work with the range of CIKR protection-related plans and programs instituted by the private sector, both through voluntary actions and as a result of various regulatory requirements. These plans and programs include business continuity and resilience measures. NIPP processes are designed to enhance coordination, cooperation, and collaboration among CIKR partners within and across sectors to synchronize related efforts and avoid duplicative or unnecessarily costly security requirements.

5.3.1 Sector-Specific Plans

Based on guidance from DHS, the SSPs were developed jointly by the SSAs in close collaboration with the SCCs, GCCs, and others, including State, local, and tribal CIKR partners with key interests or expertise appropriate to the sector. The SSPs provide the means by which the NIPP is implemented across all 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 CIKR protection programs. The SSPs for the original 17 sectors were officially released on May 21, 2007, after review and comment by the Homeland Security Council's Critical Infrastructure Protection Policy Coordination Committee. The SSP for the Critical Manufacturing Sector is under development and is scheduled for release in 2009.

Those SSPs that are available for general release may be downloaded from: http://www.dhs.gov/nipp (click on Sector-Specific Plans). If an SSP is not posted there, it is marked as FOUO. To request copies of the FOUO SSPs, please contact the responsible SSA, or the NIPP Program Management Office (NIPP@dhs.gov).

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

- Define sector partners, authorities, regulatory bases, roles and responsibilities, and interdependencies;
- Establish or institutionalize already existing procedures for sector interaction, information sharing, coordination, and partnership;
- Establish the goals and objectives, developed collaboratively among sector partners, that are required to achieve the desired protective posture for the sector;

- Identify international considerations;
- Identify areas for government action above and beyond an owner/operator or sector risk model; and
- Identify the sector-specific approach or methodology that SSAs use, in coordination with DHS and other sector partners, to conduct the following activities through the NIPP framework:
  - Identify priority CIKR and functions within the sector, including cyber considerations;
  - Assess sector risks, including potential consequences, vulnerabilities, and threats;
  - Assess and, as appropriate, prioritize assets, systems, networks, and functions of national-level significance within the sector;
  - Develop risk-mitigation programs based on detailed knowledge of sector operations and risk landscape;
  - Provide protocols to transition between steady-state CIKR protection and incident response in an all-hazards environment;
  - Use metrics to measure and communicate program effectiveness and risk management progress within the sector;
  - Address R&D requirements and activities relevant to the sector; and
  - Identify the process used to promote cooperation and information sharing within the sector.

The structure for the SSPs facilitates cross-sector comparisons and coordination by DHS and other SSAs.

5.3.2 State, Regional, Local, Tribal, and Territorial CIKR Protection Programs

The National Preparedness Guidelines define the development and implementation of a CIKR protection program as a key component of State, regional, local, tribal, and territorial homeland security programs. Creating and managing a CIKR 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 action within the jurisdiction to: set goals and objectives; identify assets, systems, and networks; assess risks; set priorities for CIKR across sectors and jurisdictional levels; implement protective programs and resiliency strategies; measure the effectiveness of risk management efforts; and share information among relevant public and private sector partners. These elements form the basis of focused CIKR protection programs and guide the implementation of the relevant CIKR protection-related goals and objectives outlined in State, local, and tribal homeland security strategies. To assist in the development of such CIKR protection programs, DHS issued a collaboratively developed Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal, and Territorial Levels (2008). The guide can be downloaded at www.dhs.gov/nipp.

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

State, regional, local, tribal, and territorial CIKR 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 CIKR protection planning activities, the basic elements to be incorporated in these efforts are provided in appendix 5A. The recommended elements described in this 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 varying authorities, resources, and issues within each State or region.

5.3.3 Other Plans or Programs Related to CIKR Protection

Federal partners should review and revise, as necessary, other plans that address elements of CIKR protection to ensure that they support the NIPP in a manner that avoids duplication and unnecessary layers of CIKR protection guidance. Examples of government plans or programs that may contain relevant prevention, protection, and response protocols or activities that relate to or affect CIKR protection include plans that address: State, local, and tribal hazard mitigation;

continuity-of-operations (COOP); continuity-of-government (COG); environmental, health, and safety operations; and integrated contingency operations. 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. Many of these plans include heightened security requirements for CIKR protection that address the terrorist threat environment. Coordination with these planning efforts is relevant to effective implementation of the NIPP. Private sector partners are encouraged to consider the NIPP when revising these plans and to work with government partners to integrate their efforts with Federal, State, local, and tribal CIKR protection efforts, as appropriate.

5.4 CIKR Protection and Incident Management

Together, the NIPP and the NRF 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-informed approach that defines the Nation's steady-state posture with respect to CIKR protection and resiliency, while the NRF 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 partnership model provide vital functions that, in turn, inform and enable incident management decisions and activities.

5.4.1 The National Response Framework

The NRF provides an all-hazards approach that incorporates best practices from a wide variety of disciplines, including fire, rescue, law enforcement, public works, and emergency medical services. The operational and resource coordinating structures described in the NRF are designed to support decisionmaking 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 NRF applies to a wide array of natural disasters, terrorist threats and incidents, and other emergencies.

The NRF core document and annexes, including the CIKR Support Annex, describe processes for coordination among various Federal departments and agencies; State, local, and tribal governments; and private sector partners, both for pre-incident preparedness, and post-incident response and short-term recovery. The NRF specifies incident management roles and responsibilities, including emergency support functions designed to expedite the flow of resources and program support to the incident area. The SSAs and other Federal departments and agencies have roles within the NRF structure that are distinct from, yet complementary to, their responsibilities under the NIPP. Ongoing implementation of the NIPP risk management framework, partnerships, and information-sharing networks sets the stage for CIKR security and restoration activities within the NRF by providing mechanisms to quickly assess the impact of the incident on both local and national CIKR, assist in establishing priorities for CIKR restoration, and augment incident-related information sharing.

5.4.2 Transitioning From NIPP Steady-State to Incident Management

The variety of alert and warning systems that exist for natural hazards, technological or industrial accidents, and terrorist incidents provide the bridge between steady-state operations using the NIPP risk management framework and incident management activities using the NRF concept of operations. These all-hazards alert and warning mechanisms include programs such as National Weather Service hurricane and tornado warnings, and alert and warning systems established around nuclear power plants and chemical stockpiles. In the context of terrorist incidents, HSAS provides a progressive and systematic approach that is used to match protective measures to the Nation's overall threat environment. This link between the current threat environment and the corresponding protective actions related to specific threat vectors or scenarios and to each HSAS threat level provides the indicators used to transition from the steady-state processes detailed in the NIPP to the incident management processes described in the NRF.

DHS and CIKR partners develop and implement stepped-up protective actions to match the increased terrorist threat conditions specified by HSAS, and to address various other all-hazards alerts and warning requirements. As warnings or threat levels increase, NRF coordinating structures are activated to enable incident management. DHS and CIKR partners carry out their NRF responsibilities and also use the NIPP risk management framework to provide the CIKR protection dimension of incident operations. The NRF CIKR Support Annex describes the concept of operations and details the activities needed to support public-private sector

incident operations and requirements, as well as to provide situational awareness, analysis, and prioritized recommendations to inform incident management decisions. When an incident occurs, regardless of the cause, the NRF is implemented for overall coordination of domestic incident management activities. The CIKR Support Annex includes a process for considering requests for assistance from CIKR owners and operators. Implementation of the CIKR Support Annex and the NIPP risk management framework facilitates those actions directly related to the current threat status, as well as incident prevention, response, and recovery. The NRF and CIKR Support Annex can be found at www.fema.gov/NRF.

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

- Increasing protection levels to correlate with the specific threat vectors or threat level communicated through HSAS or other relevant all-hazards alert and warning systems, or in accordance with sector-specific warnings using the NIPP information-sharing networks;
- Using the NIPP information-sharing networks and risk management framework to review and establish national priorities for CIKR protection; facilitating communications between CIKR partners; and informing the NRF processes regarding priorities for response and recovery of CIKR within the incident area, as well as on a national scale;
- Fulfilling roles and responsibilities as defined in the NRF for incident management activities; and
- Working with sector-level information-sharing entities and owners and operators on information-sharing issues during the active response mode.

In addition, the DHS Office of Public Affairs has an established communications protocol to facilitate timely information exchange and necessary coordination with the CIKR sectors and their Federal, State, local, and private sector partners during those national-level incidents that involve a coordinated Federal response.

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

This chapter addresses the efforts needed to ensure an effective, efficient CIKR protection program over the long term. It focuses particularly on the long-lead-time elements that require sustained plans and investments over time, such as generating skilled human capital, developing high-tech systems, and building public awareness.

Key activities needed to enhance CIKR protection and resiliency over the long term include:

- Building national awareness to support the CIKR protection program and related investments by ensuring a focused understanding of the all-hazards risk environment and what is being done to protect and enable the timely restoration of the Nation's CIKR in light of 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 and using technology to improve protective capabilities or resiliency strategies or to lower the costs of existing capabilities so that CIKR partners can afford to do more with limited budgets;
- Developing, protecting, 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

DHS, in conjunction with the SSAs and other CIKR partners, is responsible for implementing a comprehensive national awareness program that focuses on public and private sector understanding of the CIKR all-hazards risk environment and motivates actions that support the sustainability of CIKR protection, investments, and risk management initiatives. Objectives of the CIKR national awareness program are to:

- Incorporate CIKR protection and restoration considerations into business planning and operations, including employee and senior manager education and training programs, across all levels of government and the private sector;
- Support public and private sector decisionmaking; enable relevant and effective strategic planning for CIKR protection and restoration; and inform resource allocation processes;
- Foster an understanding of:
  - CIKR dependencies and interdependencies, and the value of cross-sector CIKR protection and restoration planning down to the community level;
  - Evolving threats to CIKR as assessed by the intelligence community and in the context of HSAS; and

– Efforts to address the threat environment and enhance CIKR protection, resiliency, and rapid restoration.

DHS and other Federal agencies also engage in comprehensive national cyberspace security awareness campaigns to remove impediments to sharing vulnerability information among CIKR partners. This campaign includes audience-specific awareness materials, expansion of the Stay Safe Online campaign, and development of awards programs for those making significant contributions to the effort.

A Continuum of Capability Development

This document establishes a framework to enable awareness, education, training, and exercise programs that allow people and organizations to develop and maintain the core competencies and expertise required for effective implementation of the CIKR protection mission. Building the requisite individual and organizational capabilities requires attracting, training, and maintaining sufficient numbers of professionals who have the particular expertise unique or essential to CIKR protection. This, in turn, requires individual education and training to develop and maintain the requisite levels of competency through technical, academic, and professional development programs. It also requires organizational training and exercises to validate the processes and enhance the efficiency and effectiveness of CIKR programs.

As illustrated in figure 6-1, outreach and awareness create the foundation on which a comprehensive CIKR education and training program can be built. Exercises provide an objective assessment of an entity's or individual's capabilities, thus identifying areas for improvement and highlighting training gaps and needs.

The objectives of NIPP-related training and education programs are to:

- Provide an integrated, coordinated approach to NIPP and CIKR-related education and training that energizes and involves all partners;
- Develop and implement grassroots education and training programs that communicate effectively with key audiences; and
- Maximize coordination, deepen relationships, and broaden the participation and practices required for implementing the NIPP and the SSPs.

The framework for education, training, and exercise is discussed below.

6.1.1 Education and Training

CIKR threat mitigation and protection have a broad target audience. Emphasis, for the purposes of education and training, is

Figure 6-1: Continuum of CIKR Capability Development

placed on these target audiences as collections of individuals rather than as organizations or entities, since it is the engagement and decisionmaking of those individuals, operating in their own areas of expertise and responsibility, that will determine the success of the public-private CIKR partnership.

It is crucial to understand these audiences and the similarities and differences among them in order to ensure the effective and efficient delivery of CIKR-related education and training. The following is a description of the primary CIKR training target audiences:

- State, local, tribal, and territorial government officials; SLTTGCC members; State elected officials; Homeland Security Directors and Advisors; emergency managers; program managers; and specialists;
- IP personnel, senior executives, program managers/analysts, PSAs, training managers, and specialists;
- The SSA and other Federal agency personnel; senior executives, program managers, and specialists;
- Regional consortium members;
- Owner/operator executives, security managers, program managers, and specialists; and
- Others, including international partner executives, security managers, program managers, and specialists.

6.1.2 Core Competencies for Implementing CIKR Protection

The U.S. Office of Personnel Management defines a competency as "a measurable pattern of knowledge, skills, abilities, behaviors, and other characteristics that an individual needs to perform work roles or occupational functions successfully." A competency model is a collection of competencies that together define the elements required for performance. The CIKR competency model, illustrated in figure 6-2, provides the following:

- Define education and training requirements;
- Organize existing education and training efforts;
- Identify education and training gaps;
- Set forth a business case for education and training investments; and
- Establish performance metrics.

Each competency area is defined in table 6-1, which follows figure 6-2.

Figure 6-2: Developing CIKR Core Competencies

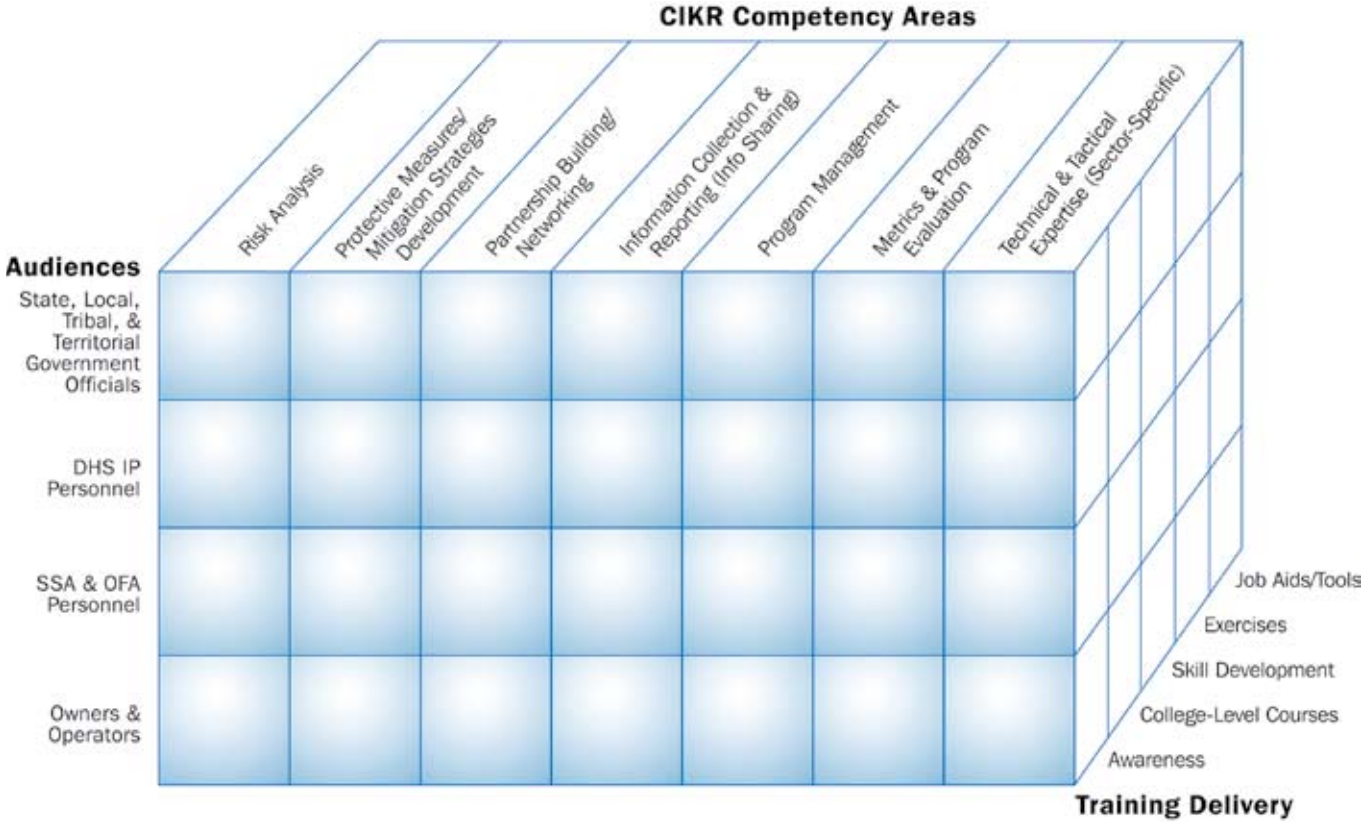


Table 6-1: CIKR Competency Areas

Area	Includes Knowledge and Skills To . . .
Risk Analysis	• Perform accurate, documented, objective, defensible, transparent, and complete analyses. • Support executive and managerial decisionmaking related to CIKR programs.
Protective Measures/ Mitigation Strategies	• Establish CIKR program goals and objectives based on risk analysis and risk-reduction return on investment. • Plan, develop, and implement CIKR-related projects, measures, and activities. Take advantage of existing emerging and anticipated methods and technologies in order to develop effective strategies, projects, and activities. • Implement continuous feedback mechanisms.
Partnership Building/ Networking	• Understand the roles and responsibilities of all partners. • Establish mechanisms for interacting with partners and exchanging information and resources (including best practices).
Information Collection & Reporting (Information Sharing)	• Use systems, tools, and protocols to collect, analyze, organize, report, and evaluate information. • Communicate and share information with sector partners at each tier of governance, including sector-specific, across sectors, and within the private sector.
Program Management	• Establish sector-specific or jurisdictional CIKR goals and plans. • Identify and prioritize CIKR projects, strategies, and activities for a sector or jurisdiction. • Manage a CIKR program on schedule, within budget, and in compliance with performance standards. • Design and implement continuous feedback mechanisms at the program level. • Develop and implement CIKR training plans.
Metrics & Program Evaluation	• Define and establish CIKR metrics based on goals and objectives. • Establish data collection and measurement plans, systems, and tools. • Collect and analyze data. • Report findings and conclusions.
Technical & Tactical Expertise (Sector- Specific)	• Note: This area includes the specialized (sector-specific) expertise required to plan, implement, and evaluate technical and tactical activities, measures, and programs.

The training delivery levels identified in figure 6-2 represent a cumulative structure that begins with basic awareness and progresses to the expert knowledge and skills required to perform specific CIKR-related tasks and functions. Training and education programs typically fall into these levels:

- **Awareness Materials**: Motivate or inform course participants about CIKR-related concepts, principles, policies, or procedures.
- **College Courses**: Present advanced CIKR knowledge, research, and theories to promote professional development.
- **Skill Development Sessions**: Focus on improving the performance of specific CIKR functions and tasks, both during training and in the workplace.
- **Exercises**: Reinforce and test CIKR skill acquisition, processes, and procedures.
- **Job Aids**: Include tools or resources (such as guides, checklists, templates, and decision aids) that allow an individual to quickly access the CIKR information that he/she needs to perform a task.

6.1.3 Individual Education and Training

Building and sustaining capabilities to implement the NIPP involves a complex approach to the education and training effort that leverages existing accredited academic programs, professional certification standards, and technical training programs. This requires an effort with a national scope that includes, but is not limited to, the following components:

- Training to provide individuals with the skills needed to perform their roles and responsibilities under the NIPP and the SSPs;
- Academic and research programs that result in formal degrees from accredited institutions; and
- Professional continuing education, which incorporates the latest advances in CIKR risk-mitigation approaches and, where appropriate, certification based on government, industry, and professional organization standards.

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

6.1.3.1 CIKR Protection Training

DHS, SSAs, and other CIKR partners offer a wide array of training programs designed to enhance core competencies and build the capabilities needed to support NIPP and SSP implementation among the various target audiences. The level and content of training programs vary based on sector requirements. Some sectors rely on the use of established training programs, while others develop courses to meet specific tactical or technical objectives. DHS offers NIPP-awareness-level training through the FEMA Emergency Management Institute (EMI). The independent study course (IS 860) is available online or for classroom delivery. This course provides a foundation of the basic principles of the NIPP, including the risk management framework and partnership model, information sharing, and roles and responsibilities.

DHS, SSAs, and other CIKR partners offer courses that enhance CIKR protection. One of the ongoing objectives of NIPP- and SSP-related training is to identify and align training that enhances the core competencies and provides the appropriate level of training and development opportunities for each of the identified training audiences.

NIPP and SSP-related training and education programs, to date, focus on enhancing risk management, information collection, and the tactical and technical competencies required to detect, deter, defend, and mitigate against terrorist activities and other incidents. DHS and other Federal agencies support and provide training resources to local law enforcement and others, with a special focus on urban areas with significant clusters of CIKR, localities where high-profile special events are typically scheduled, or other potentially high-risk geographical areas or jurisdictions. Federally provided technical training covers a range of topics such as buffer zone protection, bombing prevention, workforce terrorism awareness, surveillance detection, high-risk target awareness, WMD incident training, and continuity-of-operations training.

DHS supports cybersecurity training, education, and awareness programs by educating vendors and manufacturers on the value of: pre-configuring security options in products so that they are secure on initial installation; educating users on secure 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 guidelines. These training efforts also encourage programs that leverage the existing Federal Cyber Service: 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, as required.

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

6.1.3.2 Academic Programs

DHS works with a wide range of academic institutions to incorporate CIKR protection into professional education programs with majors or concentrations in this mission area. DHS collaborates with universities to incorporate homeland security-related curriculum, sponsors a post-graduate level program at the Naval Postgraduate School in homeland defense and security, and collaborates with other higher education programs. These venues offer opportunities to incorporate concentrations in various aspects of CIKR protection as part of the multidisciplinary degree programs.

DHS is promoting the development of a long-term higher education program that will include academic degrees and adult education. The program is being developed through a collaborative effort involving the IP, the S&T Universities and Centers for Excellence Programs, TSA, and others. The initial program is being developed in conjunction with the National Transportation Security Center for Excellence (NTSCOE), which brings together a number of academic institutions with a mandate to build education and training programs relevant to the CIKR protection mission. This initiative provides the framework for the identification, development, and delivery of critical infrastructure courses for the transportation industry. The initiative will lead to the implementation of adult education and academic degree programs as part of a multidisciplinary core curriculum applicable across all critical infrastructure sectors.

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

- Co-sponsorship of the National Centers of Academic Excellence in Information Assurance Education (CAEIAE) and CAE research programs with the National Security Agency; and
- Collaboration with the National Science Foundation to co-sponsor the Federal Cyber Service: Scholarship for Service Program. The Scholarship for Service Program provides grant money to selected CAEIAE universities to fund the final 2 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 R&D Plan appropriately considers the human capital needs for protection-related R&D by incorporating analysis of the research community's future need for advanced degrees in protection-related disciplines into the plan development process.

6.1.3.3 Continuing Education and Professional Competency

DHS encourages the use of established professional standards where practical and, when appropriate, works with CIKR partners to facilitate the development of continuing education, professional competency programs, and professional standards for areas requiring unique and critical CIKR protection expertise. For example, DHS is fostering the development of CIKR adult and continuing education programs and leading the development of private sector preparedness standards that are relevant to the CIKR protection mission.

The adult education initiative focuses on enhancing the skills and abilities of CIKR professionals and employees at all levels in order to provide:

- General awareness and baseline understanding of critical infrastructure, preparedness, and protective measures; and
- Specialized CIKR training for individuals directly engaged in jobs or activities related to CIKR protection (security, business continuity, emergency management, IT, engineering, and others).

6.1.4 Organizational Training and Exercises

Building and maintaining organizational and sector expertise requires comprehensive exercises to test the interaction between the NIPP and the NRF in the context of terrorist incidents, natural disasters, and other emergencies. Exercises are conducted by 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 the NEP. Through the NEP Training and Exercise Planning Workshop, CIKR exercises can be nominated for inclusion on the NEP Five-Year Exercise Schedule. IP, in collaboration with the SSAs and the CIKR Cross-Sector Council, serves as the conduit for all 18 CIKR sectors' participation in NEP-sponsored activities and events. As such, the IP exercise program strictly adheres to the tenets of the NEP. CIKR-related exercise planning and NIPP partner participation is coordinated within IP through its Exercise Working Group (EWG), which consists of representation from all IP projects, the SSAs, and the private sector. The EWG allows NIPP partners to translate goals and priorities into specific objectives, coordinate exercise activities, participate in the planning and conduct of exercises, and track improvement plan actions against current capabilities, training, and exercises. This group is also responsible for maintaining the IP Multi-Year Training and Exercise Plan. This document is assessed and revised, as needed, on an annual basis at the IP Training and Exercise Planning Workshop.

National Exercise Program

DHS provides overarching coordination for the NEP 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 NRF.

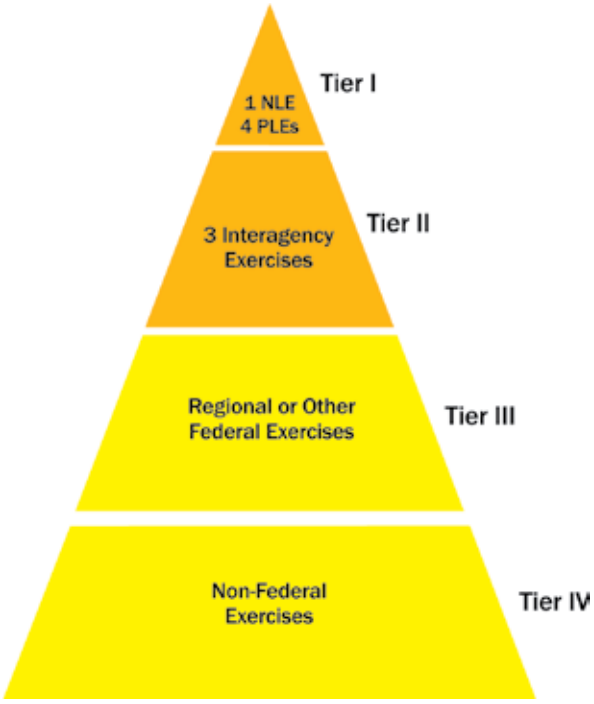
Terms used by the NEP program include:

- **National Level Exercise (NLE)**—an annual national security and/or homeland security exercise centered on White House-directed, U.S. Government-wide strategy and policy.
- **Principal Level Exercise (PLE)**—a quarterly exercise, for appropriate department and agency principals or their deputies, focused on current U.S. Government-wide strategic issues.
- **NEP Five-Year Exercise Schedule**—identifies the strategic focus and scenario of each NEP Tier 1 and II exercise that includes a strategic U.S. Government-wide focus.
- **National Exercise Schedule (NEXS)**—a schedule of all Federal, State, and local exercises.
- **Corrective Action Program (CAP)**—administered by DHS in support of the Homeland Security Council (HSC) and the National Security Council (NSC), involves a system and process for identifying, assigning, and tracking the remediation of issues.
- **Homeland Security Exercise and Evaluation Program (HSEEP)**—DHS policy and guidance for designing, developing, conducting, and evaluating exercises. Provides a threat and performance-based exercise process that includes a mix and range of exercise activities through a series of four reference manuals to help States and local jurisdictions establish exercise programs and design, develop, conduct, and evaluate exercises.

The NEP categorizes exercise activities into four tiers, as shown in figure 6-3. These tiers reflect the relative priority for national and regional Federal interagency participation, with NEP Tier I as the highest and NEP Tier IV as the lowest. U.S. Government exercises are assigned to NEP tiers based on a consensus interagency judgment of how closely they align to U.S. Government-wide strategic and policy priorities.

- **Tier I Exercises (Required)**: NEP Tier I exercises are centered on White House directed, U.S. Government-wide strategy and policy-related issues and are executed with the participation of all appropriate department and agency principals (or their deputies) and all necessary operations centers, nationally and regionally as appropriate. NLEs and Principal-Level Exercises (PLEs) constitute NEP Tier I and there are five NEP Tier I exercises annually.

Figure 6-3: National Exercise Program Tiers



- **Tier II Exercises (Commended)**: NEP Tier II exercises are focused on strategy and policy issues supported by all appropriate departments and agencies, either through the National Exercise Simulation Cell or as determined by each department or agency's leadership. NEP Tier II exercises are endorsed through the NEP process as meriting priority for interagency participation. NEP Tier II exercises take precedence over NEP Tier III exercises in the event of resource conflicts. The Exercise and Evaluation Sub-Policy Coordination Committee shall recommend no more than three NEP Tier II exercises for interagency participation annually.
- **Tier III Exercises (Permitted)**: NEP Tier III exercises are other Federal exercises focused on plans, policies, procedures, and objectives at the operational, tactical, or organization-specific level that do not require broad interagency headquarters-level involvement to achieve their stated exercise or training objectives.
- **Tier IV Exercises**: NEP Tier IV exercises are exercises in which State, local, tribal, and/or territorial governments, and/or private sector entities are the primary training audience or the subject of evaluation.

DHS chairs and facilitates the NEP Executive Steering Committee (ESC). The NEP ESC coordinates department and agency, as well as regional, State, and local exercise requirements and objectives, and builds a recommended NEP Five-Year Exercise Schedule. The NEP ESC also prioritizes recommended lessons learned and corrective action plans. The core members include DHS, DoD, DOE, HHS, DOJ, DOS, DOT, the Office of the Director of National Intelligence (ODNI), and the FBI. There are up to three rotating members serving 1-year terms. HSC, NSC, and OMB representatives serve in a non-voting oversight capacity. The recommended NEP Five-Year Exercise Schedule and CAP are submitted to the Deputies for approval through the Domestic Response Group Exercise and Evaluation Policy Coordination Subcommittee to frame those decisions.

Capabilities-Based Planning

The NEP has adopted a capabilities-based approach to exercise program management, foundation, design, development, conduct, evaluation, and improvement planning. Capabilities-based planning builds capabilities suitable for a wide range of threats and hazards while working within an economic framework that necessitates prioritization and choice. It addresses uncertainty by analyzing a wide range of realistic scenarios to identify required capabilities, and is the basis for guidance such as the National Preparedness Guidelines, Target Capabilities List (TCL), and Universal Task List (UTL). Capabilities-based planning is incorporated throughout the cycle of preparedness, to include plans, training, equipment, as well as exercises.

Training and Exercise Outreach and Coordination

DHS, SSAs, SCC, GCC, owners and operators, and other CIKR partners work together to ensure that exercises include adequate testing of steady-state CIKR protection measures and plans, including: information sharing; application of the NIPP risk management framework; and the ability of a protected core of life-critical CIKR 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 also ensures that the NIMS Integration Center, which serves as the repository and clearinghouse for reports and lessons learned from actual incidents, training, and exercises, regularly compiles and disseminates information on CIKR protection best practices.

In an effort to better familiarize its State, regional, local, tribal, territorial, and private sector partners with the NIPP, IP hosts an annual series of NEP Tier III, NIPP-related workshops and tabletop exercises. The goals for this series include increasing the understanding of: the NIPP; the IP organization, as well as non-IP SSAs; IP critical points of entry for public and private partners; State, regional, local, tribal, and territorial organizations' CIKR protection programs; and private sector CIKR protection activities, as well as identifying gaps and redundancies in these CIKR protection efforts.

6.1.5 CIKR Partner Role and Approach

Given the scope and nature of the education, training, and exercise needs related to CIKR protection, the approach adopted must, to the greatest extent possible, leverage existing education, training, and exercise programs.

DHS works through the NIPP partnership structure to provide awareness-level training to introduce public and private sector partners to the NIPP contents and requirements, and other core curriculum that provides a cross-sector basis for CIKR program management, sector awareness, metrics, and other content relevant for all sectors and jurisdictions. DHS encourages and, where appropriate, facilitates specialized NIPP-related occupational and professional training and education, and development of professional and personnel security guidelines. It also will encourage academic and research programs, and coordinate the design of exercises that test and validate the interaction between the NIPP framework and the NRF.

The SSAs and other Federal agencies are responsible for reviewing, updating, and, as appropriate, developing new CIKR protection-related training and education programs that align with the NIPP and the competency model. Other CIKR partners are encouraged to review existing training and/or develop new training to align with the competency model and support implementation of the NIPP, the SSPs, and/or identified CIKR protection needs within their jurisdiction. All CIKR partners should work with DHS and the SSAs to identify and fill gaps in current training, education, and exercise programs for those specialized disciplines that are unique to CIKR protection and resiliency.

6.2 Conducting Research and Development and Using Technology

HSPD-7 establishes the national policy for "enhancing protection of the Nation's critical infrastructure and key resources" and mandates plans to: systematically "harness the Nation's research and development capabilities"; provide the long-term technology advances needed for more effective and cost-efficient protection of CIKR; and provide the sustained science, engineering, and technology base needed to prevent

or minimize the impact of future attacks on our physical and cyber infrastructure systems.

Protection of the Nation's physical and cyber infrastructure and the people who operate and use these vital systems is an extremely challenging portion of the overall homeland security effort. The national architecture of CIKR assets and systems continually grow more complex and more interdependent. Therefore, plans must cut across a broad range of sectors, Federal and non-Federal governmental entities, and critical industries.

Federal agencies work collaboratively to design and execute R&D programs to help develop knowledge and technology that can be used to more effectively mitigate the risk to CIKR. Congress has provided for liability protections under the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act) that serve to encourage technology use by CIKR partners.

In the near term, risk-informed priorities are designed to allocate resources where they can best mitigate risk or improve resiliency. In the long term, R&D holds the key to more effective and cost-efficient CIKR protection and resiliency through advances in technology. R&D programs work to improve all aspects of CIKR protection—from the detection of threats, through protection and performance measures, to inherently secure and more resilient advanced infrastructure designs.

Because owners and operators play a major role in CIKR protection, research programs that support the NIPP must find effective ways to consider the perspectives of sector professional associations, sector councils, and other sources that understand owner and operator technology needs.

Unique R&D needs associated with CIKR protection include:

- Conducting the development or redesign of technology-based equipment to significantly lower the costs of existing capabilities so that CIKR partners with limited budgets can afford state-of-the-art solutions;
- Researching issues, such as resiliency and protection in building design, that affect all CIKR and can result in solutions that can provide benefits across sectors if implemented; and
- Focusing research on the implementation and operational aspects of technology used for CIKR protection to provide resources that can help inform technology investment decisions, such as technical evaluation of security equipment or technology clearinghouse information.

6.2.1 The SAFETY Act

Ingenuity and invention are the lifeblood of robust R&D. But potential liabilities could stifle the entrepreneurial spirit for developing technologies and products that disrupt attacks and enable effective response. As part of the Homeland Security Act, Public Law 107-296, Congress enacted the SAFETY Act, which creates liability protections for sellers of qualified anti-terrorism technologies. The SAFETY Act provides incentives for the development and deployment of anti-terrorism technologies by limiting liability through a system of risk and litigation management. The purpose of the SAFETY Act is to ensure that the threat of liability does not deter potential sellers of anti-terrorism technologies from developing, deploying, and commercializing technologies that could save lives. The SAFETY Act gives liability protection to both sellers of qualified anti-terrorism technology and their customers, and applies to all types of enterprises that develop, sell, or use anti-terrorism technologies.

The SAFETY Act applies to a broad range of technologies, including products, services, and software, or combinations thereof, as well as technology firms and providers of security services. The SAFETY Act protects those businesses and their customers and contractors by providing a series of liability protections if their products or services are found to be effective by the Secretary of Homeland Security. Additionally, if the Secretary certifies the technology under the SAFETY Act (i.e., that the technology actually performs as it is intended to do and conforms to certain seller specifications), the seller is afforded a complete defense in litigation related to the performance of the technology in preventing, detecting, or deterring terrorist acts or deployment to recover from one. Those technologies that have been "certified" are placed on an Approved Product List for Homeland Security that is available at www.safetyact.gov.

A clear benefit of the SAFETY Act is that a cause of action may be brought only against the seller of the Qualified Anti-Terrorism Technology and may not be brought against the buyer(s), their contractors, or downstream users of the Qualified Anti-Terrorism Technology, or against the seller's suppliers or contractors. This stipulation includes CIKR owners and operators.

CIKR facility owners and operators are encouraged to examine the SAFETY Act closely because: (1) CIKR owners (if purchasers of qualified technologies) will enjoy the liability protections that flow from using qualified SAFETY Act technologies, and (2) CIKR owners will also have a level of assurance that the qualified products and services that

they are utilizing have been vetted by DHS. Lower liability insurance burdens for those using qualified technologies are another potential outcome.

In these ways, the SAFETY Act is a valuable tool that can enhance the ability of owners and operators to protect our Nation's CIKR.

6.2.2 National Critical Infrastructure Protection R&D Plan

As directed by HSPD-7, the Secretary of Homeland Security works with the Director of OSTP, EOP, to develop the NCIP R&D Plan as a vehicle to support implementation of CIKR risk management and supporting activities and programs.

The NCIP R&D Plan provides the focus and coordination mechanisms required to achieve the vision provided in the President's Physical and Cyber Security CIKR 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 partners and to 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 CIKR protection. The planning process also provides for the revision of research goals and priorities over the long term to respond to changes in the threat, technology, environment, business continuity, and other factors.

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

The NCIP R&D Plan articulates strategic R&D goals and identifies the R&D areas in which advances in CIKR protection must be made. The goals and cross-sector R&D areas contained in the NCIP R&D Plan are discussed in the following subsections.

6.2.2.1 CIKR Protection R&D Strategic Goals

The NCIP R&D planning process identifies three long-term, strategic R&D goals for CIKR protection:

- A common operating picture to continuously monitor the health of CIKR;
- A next-generation Internet architecture with designed-in security; and
- Resilient, self-diagnosing, self-healing infrastructure systems.

The strategic goals are used to guide Federal R&D investment decisions and also to provide a coordinated approach to the overall Federal research program. S&T and OSTP will work with OMB to use the R&D Plan as a decisionmaking tool for the evaluation of budget submissions across Federal agencies. These goals also help guide the programs of researchers who receive Federal grants and contracts.

6.2.2.2 CIKR Protection R&D Areas

R&D development projects for CIKR protection programs fall into nine R&D areas or themes that cut across all CIKR sectors:

- Detection and sensor systems;
- Protection and prevention systems;
- Entry and access portals;
- Insider threats;
- Analysis and decision support systems;
- Response and recovery tools;
- New and emerging threats and vulnerabilities;
- Advanced infrastructure architectures and systems design; and
- Human and social issues.

Organizing research in these areas enables the development of effective solutions that may be applied across sectors and disciplines. These themes also provide an organizing framework for SSA use during the development of R&D requirements for their respective sectors, which will be reflected in the SSPs. These requirements specify the capabilities that each sector needs to satisfy CIKR 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 CIKR Protection. Requirements are refreshed each year through the sector annual reporting process.

6.2.2.3 Coordination of the NCIP R&D Plan With SSP and Sector Annual Report R&D Planning

Each SSP includes a section on sector-specific CIKR protection R&D that explains how the sector will strengthen the linkage among sector-specific and national R&D planning efforts, technology requirements, current R&D initiatives, gaps, and candidate R&D initiatives. New candidate R&D initiatives are developed during the Sector Annual Report writing process. The SSP explains the process for:

- **Sector Technology Requirements**: Identifying and providing a summary of sector technology requirements and communicating them to IP, S&T, and 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 S&T and OSTP that have the potential to meet sector CIKR 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 S&T and OSTP; and
- **Candidate R&D Initiatives**: Determining which candidate R&D initiatives are most relevant for the sector and how these will be summarized and reported to all appropriate stakeholders.

Each SSA coordinates the development of the sector R&D planning component of their SSP and SAR so that these documents reflect the SSA's sector-level R&D investment priorities. Coordination between IP, S&T, and the sectors through the SSAs, GCCs, and SCCs ensures that the R&D information in the SSP and Sector Annual Report is comprehensive.

6.2.3 Other R&D That Supports CIKR Protection

Other R&D efforts that may support CIKR protection are conducted by the SSAs and other Federal agencies. These programs address the research requirements set forth in the President's Physical and Cyber Security CIKR 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 CIKR protection consensus standards; and
- Improving technological surveillance, monitoring, and detection capabilities.

For example, the Technical Support Working Group is the U.S. national forum that identifies, prioritizes, and coordinates interagency and international R&D requirements for combating terrorism. The Technical Support Working Group rapidly develops technologies and equipment to meet the high-priority needs of the anti-terrorism community, including efforts that can contribute to CIKR protection, and addresses joint international operational requirements through cooperative R&D with major allies.

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

6.2.4 DHS Science and Technology Strategic Framework

The Homeland Security Act of 2002 gave S&T the responsibility of advising the DHS Secretary on S&T requirements, priorities, and programs that support the department's vision and mission. The directorate also has the responsibility of developing and integrating technology with the strategies, policies, and procedures in order to protect the Nation's CIKR.

CIKR requirements are mapped to Integrated Product Teams (IPTs) managed by S&T. S&T focuses on enabling its customers—the DHS components—and their customers, including: Border Patrol agents; the Coast Guard; airport baggage screeners; Federal Air Marshals; and State, local, and Federal emergency responders, as well as the many others teamed and committed to the vital mission of securing the Nation. Other CIKR customers of S&T are the sectors and their partners who own and operate infrastructure. Sectors develop long-term requirements that are documented in SSPs. Sector Annual Reports update requirements in response to changes in risk as advised by the annual National Risk Profile. The National Annual Report further applies the National Risk Profile to prioritize requirements across sectors.

To reach its goals, S&T created a customer-focused, output-oriented, full-service S&T management organization. See appendix 6 for a detailed discussion of the S&T organization as it relates to CIKR technology development.

6.2.5 Transitioning Requirements Into Reality

After identifying and justifying risk-based R&D requirements in the Sector CIKR Protection Annual Reports, the full set of requirements are reviewed, summarized, and consolidated to develop the set presented in the National CIKR Protection Annual Report. DHS works with the SSAs, SCCs, GCCs, and cross-sector councils to further validate and refine the requirements and to prioritize them before submitting them

to the IPT process. The different IPTs then work to define the actual projects, identify costs and resources, and finally turn them into S&T projects.

Specifically, IPTs coordinate the planning and execution of R&D programs together with the eventual hand-off to the maintainers and users of the project results. The IPTs are critical nodes in the process to determine operational requirements, assess current capabilities to meet operational needs, analyze gaps in capabilities and articulate programs and projects to fill in the gaps and expand competencies.

IPTs constitute the Transition portfolio of S&T, targeting deployable capabilities in the near term. IPTs generally include the research and technology perspective, the customer/end-user perspective, and an acquisitions perspective. The customers/end-users monitor and guide the capability being developed; the research and technology representatives inform the discussions with scientific and engineering advances and emerging technologies; and the acquisitions staff helps to transition the results into practice by the maintainers and the end-users of the capability.

The overall requirements process promotes rigor in the analysis and prioritization of sector requirements and capability gaps and also provides feedback to sectors on how their needs align with ongoing and planned S&T projects.

6.3 Building, Protecting, and Maintaining Databases, Simulations, and Other Tools

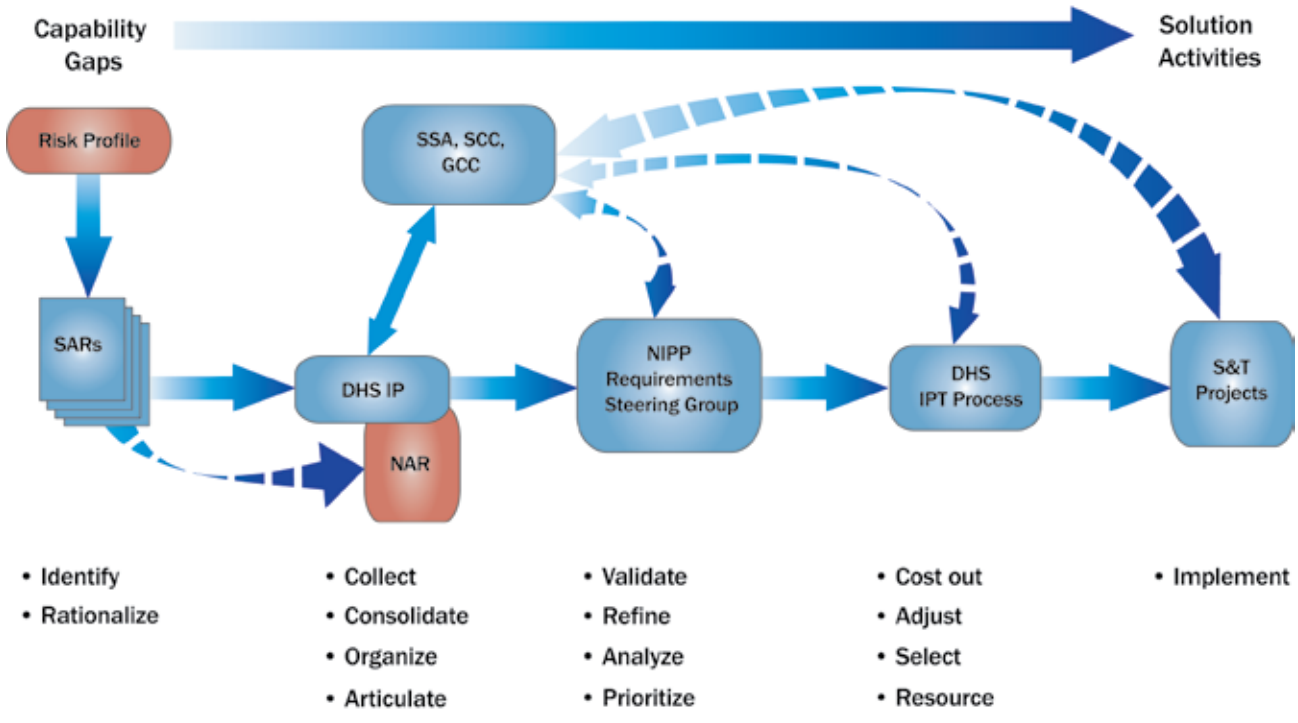
Many data systems, databases, models, simulations, decision support systems, and similar information tools currently exist or are under development to enable the execution of national CIKR risk management.

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. Sensitive information associated with these tools must be appropriately protected. Priority efforts in this area will be focused on updating and improving key databases, developing and maintaining simulation and modeling capabilities, and coordinating with CIKR partners on databases and modeling.

6.3.1 National CIKR Protection Data Systems

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

Figure 6-4: The NIPP R&D Requirements Generation Process



- Maintaining an inventory of asset information and estimating the potential consequences of an attack or incident (e.g., the IDW);
- Storing information related to terrorist attacks or incidents (e.g., the National Threat and Incident Database);
- Analyzing dependencies and interdependencies (e.g., the NISAC);
- Managing the implementation of various protective programs (e.g., the BZPP Request Database); and
- Providing the continuous maintenance and updates required to enable data in these systems to reflect changes in actual circumstances, using tools such as iCAV and DHS Earth.

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 partners.

6.3.2 Simulation and Modeling

A number of CIKR partners make use of models and simulations to comprehensively examine the potential consequences from terrorist attacks, natural disasters, and manmade accidents that affect CIKR, including the effects of sector and cross-sector dependencies and interdependencies. Continuous maintenance and updates 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.

IP is the lead coordinator for modeling and simulation capabilities regarding CIKR protection and resiliency. In this capacity, DHS will:

- Coordinate with the S&T on requirements for the development, maintenance, and application of research-related modeling capabilities for CIKR protection and resiliency;
- Specify requirements for the development, maintenance, and application of operations-related modeling capabilities for CIKR protection in coordination with S&T and the SSAs, as appropriate;
- Coordinate with the SSAs that have relevant modeling capabilities to develop appropriate mechanisms for the development, maintenance, and use of such for CIKR protection as directed by HSPD-7;
- Familiarize the SSAs and other CIKR partners with the availability of relevant modeling and simulation capabilities through training and exercises;
- Work with end-users to design operations-related tools that provide maximum utility and clarity for CIKR protection activities in both emergencies and routine operations;
- Work with end-users to design appropriate information protection plans for sensitive information used and produced by CIKR protection modeling tools;
- Provide guidance on the vetting of modeling tools to include the use of private sector operational, technical, and business expertise, where appropriate; and
- Review existing private sector modeling initiatives and opportunities for joint ventures to ensure that DHS, the SSAs, and their CIKR partners make the maximum use of applicable private sector modeling capabilities.

The principal modeling, simulation, and analysis capability within the IP is the NISAC. NISAC analysts and operational resources are located at the Sandia and Los Alamos National Laboratories and the program operates under the direction of a Washington, DC-based program office within IP. Mandated by Congress to be a "source of National Expertise to address critical infrastructure protection" research and analysis, NISAC prepares and shares analyses of CIKR, including their interdependencies, vulnerabilities, the consequences of loss, and other complexities. NISAC has developed tailored analytical tools, a core of unique expertise, and procedures designed to effectively address the strategic-level analytical needs of CIKR decisionmakers.

While the 2001 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act established the requirement for NISAC, the Homeland Security Appropriations Act of 2007 specifies its current mission. NISAC is required to provide "modeling, simulation, and analysis of the assets and systems comprising CIKR in order to enhance preparedness, protection, response, recovery, and mitigation activities." The center is also directed to share information with Federal agencies and departments that have CIKR responsibilities. Information sharing is accomplished through outreach meetings with sectors, analysts, and consumers. NISAC pre-incident studies (e.g., hurricane scenario studies) are posted and available for downloading on HSIN. Selected products are reproduced for widespread dissemination in hard copy. Products requested from the NISAC program office are usually distributed by email or via electronic media.

NISAC's objectives cover two main areas of focus:

- Provide operational support to DHS and other Federal Government entities on an as needed basis in the form of analysis, simulation, and scenario development; and
- Develop long-term capabilities by maintaining expertise in the application of analysis tools and the development of improved processes and tools in support of longer-term DHS projects.

NISAC accomplishes its mission through three types of products:

- Pre-planned, long-term analyses;
- Pre-planned, short-term analyses; and
- Unplanned, priority analytical projects that are based on higher-level tasking or that are related to current threats to CIKR (e.g., hurricane CIKR impact analysis).

Pre-planned analyses may result from several processes, but they result primarily from the National and Sector CIKR Protection Annual Reports, along with the supporting annual reports for IP, DHS' Office of Cybersecurity and Communications (CS&C), the SLTTGCC, and the RCCC. These reports identify requirements for the analyses, which are then prioritized in a similar manner to the R&D requirements.

NISAC utilizes CIKR information and data from a variety of government CIKR sector and private sector sources, including other participants in CIKR protection projects and programs. NISAC uses some data that are considered proprietary to a single industry or even to a specific firm; the data must therefore be protected from unrestricted dissemination in order to maintain the trust of the information providers. NISAC products principally serve government decisionmakers, who can derive valuable insight into incident consequences at a higher level than the supporting data could provide. In selected cases, NISAC products are made available to the private sector in order to facilitate access to key NISAC recommendations of concern to a wider community of CIKR stakeholders.

Although NISAC is the principal resource within IP for modeling, simulation, and analysis, it is not the sole source available to CIKR stakeholders in need of these capabilities. NISAC works with other stakeholders to share critical authoritative data in order to improve overall analytical quality and ensure consistency with other providers of CIKR analysis.

6.3.3 Coordination on Databases and Modeling

Integrating existing databases into DHS databases, such as the IDW, not only reduces the duplication of effort, but also ensures that available data are consistent, current, and accurate, and provide users with a consolidated picture across all CIKR sectors. However, this approach is effective only if the source information is protected and maintained properly. Maintaining a current and useful database involves the support, coordination, and commitment of the SSAs, private sector entities, and other partners. Because the most current and accurate CIKR-related data are best known by owners and operators, the effectiveness of the effort depends on all CIKR 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:

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

DHS works with the SSAs and other CIKR partners to:

- Identify databases and other data services that will be integrated into CIKR databases and data systems;
- Facilitate the actual integration of supporting databases or the importation of data into CIKR protection databases and data systems using a common, standardized format, data scheme, and categorization system or taxonomy specified by DHS in coordination with the SSAs; and
- Define, as appropriate, the schedule for integrating data and databases into such systems as the IDW.

6.4 Continuously Improving the NIPP and the SSPs

The NIPP uses the SCCs, GCCs, and the cross-sector councils 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 the SSPs.

6.4.1 Management and Coordination

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

The NIPP is a multi-year plan describing mechanisms for sustaining the Nation's steady-state CIKR protection posture. The NIPP and its component SSPs include a process for: annual review; periodic interim updates as required; and regularly scheduled partial reviews and re-issuance every 3 years or more frequently, if directed by the Secretary of Homeland Security.

IP oversees the review and maintenance process for the NIPP; the SSAs, in coordination with the GCCs and SCCs, establish and operate the mechanism(s) necessary to coordinate this review for their respective SSPs. The NIPP and SSP revision processes includes developing or updating any documents necessary to carry out NIPP activities. The NIPP is reviewed at least annually to:

- Ensure that the NIPP framework is capable of measuring accomplishments in support of CIKR protection goals and objectives, and supporting the overall national approach to the homeland security mission;
- Ensure that the plan adequately reflects the organization of DHS and the SSAs;
- Ensure that the NIPP is consistent with the Federal plans and activities that it directly supports;
- Adjust practices and procedures called for in the NIPP based on changes in the national risk management environment;
- Incorporate lessons learned and best practices from day-to-day operations, exercises, and actual incidents and alerts; and
- Reflect progress in the Nation's CIKR protection, as well as changes to national priorities and guidance, critical tasks, sector organization, or national capabilities.

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.

6.4.2 Maintenance and Updates

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

- **Types of Changes**: Changes include the addition of new or supplementary material and deletions. No proposed change should contradict or override authorities or other plans contained in a 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 the SSAs and other CIKR partners, as appropriate. Policy changes will be coordinated and approved thorough the Homeland Security Council policy process.
- **Notice of Change**: DHS will issue an official Notice of Change for each interim revision to the NIPP. After publication, the modifications will be considered part of the NIPP for operational purposes pending a formal revision and re-issuance of the entire document. Interim changes can be further modified or updated using this process. (Periodic updates resulting from the annual review process do not require the formal Notice of Change.)
- **Distribution**: DHS will distribute Notices of Change to SCCs, GCCs, and other CIKR partners. Notices of Change to other organizations will be provided upon request.
- **Re-Issuance**: DHS will coordinate full reviews and updating of the NIPP every 3 years or more frequently, if directed by the Secretary of Homeland Security. The review and updating process will consider lessons learned and best practices identified during implementation in each sector and will incorporate the periodic changes and any new information technologies. DHS will distribute revised NIPP documents for interagency review and concurrence through the Homeland Security Council process.

The SSAs, in coordination with their GCCs and SCCs, establish and operate the mechanism(s) necessary to coordinate the SSP maintenance and update process in accordance with the process established for the NIPP.

7. Providing Resources for the CIKR Protection Program

Since the terrorist attacks of September 11, 2001, government and private sector expenditures to improve CIKR protection and resilience have increased across sectors and governmental jurisdictions. With finite resources available to support CIKR protection requirements, the NIPP serves as the unifying framework to ensure that CIKR investments are coordinated and address the highest priorities, based on risk, to achieve the homeland security mission and ensure the continuity of the essential infrastructure and services that support the American government, economy, and way of life. Where regulations require the use of certain tools, techniques, reporting, etc., the NIPP risk management framework is flexible enough to be implemented in a manner that supports those requirements.

This chapter describes an integrated, risk-informed approach to: guide resource support for the national CIKR protection program; focus Federal grant assistance to State, local, tribal, and territorial entities; and complement relevant private sector activities. This integrated approach coordinates CIKR protection programs and activities conducted by DHS, the SSAs, and other Federal entities through the Federal appropriations process, and focuses Federal grant funds to support national CIKR protection efforts conducted at the State, local, tribal, and territorial levels. This approach also includes mechanisms to involve private sector partners in the planning process and supports collaboration among CIKR partners to establish priorities, define requirements, share information, and maximize the use of finite resources. Implementation of this coordinated approach will help ensure that limited resources are applied efficiently and effectively to address the Nation's most critical CIKR protection needs.

7.1 The Risk-Informed Resource Allocation Process

Funding in support of CIKR protection programs at all levels is guided by a straightforward principle: Resources must be directed to the areas of greatest priority to enable effective management of risk. By definition, all CIKR assets, systems, and networks are important. However, considering the risk factors of threat, vulnerability, and consequences, some assets, systems, networks, or functions are more critical to the Nation, as a whole, than others. This chapter describes a process to ensure that the Nation's CIKR protection resource requirements are correctly identified and appropriately prioritized to meet the most critical protection needs as well as any relevant regulatory or congressional requirements. Using a risk-informed approach, DHS collaborates with CIKR partners to identify those assets, systems, networks, and functions that are the most critical from a national perspective and lead, integrate, and coordinate a cohesive effort to help ensure their protection and resiliency. Through the NIPP framework, DHS works with the SSAs, States, and other government and private sector partners to gain an understanding of how CIKR protection is being conducted across the country, the priorities and requirements (NIPP-based or other) that drive these efforts, and how such efforts are funded. This assessment helps DHS to identify duplicative efforts and gaps across sectors and jurisdictions. DHS then uses the information gained to recommend targeted investment that helps ensure that government resources are allocated to the

areas of the greatest priority with a view toward ensuring that investments are cost-effective in reducing risk.

7.1.1 Sector-Specific Agency Reporting to DHS

Given their unique capabilities and individual risk landscapes, CIKR sectors each face different challenges. For instance, some sectors have distinct, easily identifiable assets that can be logically prioritized. Some are characterized by thousands of distributed assets, not all of which are equally critical. Others are made up of systems or networks for which the identification of specific protective measures may prove to be extremely complex, but should be attempted nonetheless. Furthermore, interdependencies among sectors can cause duplicative efforts or lead to gaps in funding for CIKR protection. To ensure that government resources are allocated according to national priorities and are based on national risk, need, and effective risk-reduction opportunities, DHS must be able to accurately assess priorities, requirements, and efforts across these diverse sectors. Requirements driven by regulations, statutes, congressional mandates, and presidential directives should also be considered.

As DHS conducts this assessment, the SSAs, supported by their respective SCCs and GCCs, provide information regarding their sectors' individual CIKR protection efforts. The SCCs participate in the process to ensure that private sector input is reflected in SSA reporting on sector priorities and requirements. The first step for an SSA in the risk-informed resource allocation process is to coordinate with sector partners, including SCCs and GCCs, as appropriate, to determine sector priorities, program requirements, and resource needs for CIKR protection. HSPD-7 requires each SSA to provide an annual report to the Secretary of Homeland Security on their efforts to identify, prioritize, and coordinate CIKR protection and resiliency in their respective sectors. Consistent with this requirement, DHS provides the SSAs with reporting guidance and templates that include requests for specific information, such as CIKR protection priorities, requirements, and resources. The following elements are included in the Sector CIKR Protection Annual Report to help inform the prioritization of resource allocation recommendations:

- Priorities and annual goals for CIKR protection and resiliency, as well as associated gaps;
- Sector-specific requirements for CIKR protection and resiliency activities and programs based on risk, need, and any other drivers such as regulations and presidential directives;
- Projected CIKR-related resource requirements for the sector, with an emphasis on anticipated gaps or shortfalls in funding for sector- or national-level CIKR protection and resiliency; and
- CIKR, the disruption of which would cause regionally or nationally significant impacts under both steady-state and incident conditions.

7.1.2 State Government Reporting to DHS

Like sectors, State governments face diverse CIKR protection challenges and have different priorities, requirements, and available resources. Furthermore, State CIKR protection efforts are closely intertwined with those of other government and private sector partners. In particular, States work closely with local and tribal governments to address CIKR protection challenges at those levels. To accurately assess the CIKR protection effort and identify needs that warrant attention at a national level, DHS must aggregate information across State jurisdictions as it does across sectors.

DHS requires that each State develop a homeland security strategy that establishes goals and objectives for its homeland security program, which includes CIKR protection as a core element. State administrative agencies develop a Program and Capability Enhancement Plan that prioritizes statewide resource needs to support this program. The State administrative agency works with DHS to identify:

- Priorities and annual goals for CIKR protection and resiliency;
- State-specific requirements for CIKR protection activities and programs, based on risk and need;
- Mechanisms for coordinated planning and information sharing with government and private sector partners;
- CIKR, the disruption of which would cause regionally or nationally significant impacts for both steady-state and incident management purposes;
- Unfunded CIKR protection initiatives or requirements that should be considered for funding using Federal grants (described in further detail below); and
- Other funding sources utilized to implement the NIPP and address identified priorities and annual goals.

For consideration in the deliberations related to the Federal budget cycle, information on statewide CIKR resource needs must be reported to DHS by the date specified in the annual DHS Grant Programs Directorate (GPD) planning guidance. GPD includes report templates and planning guidance to support the States' reporting efforts.

7.1.3 State, Local, Tribal, and Territorial Government Coordinating Council Reporting to DHS

The intent of the SLTTGCC is to provide input and suggestions for implementation of the NIPP, including sector protection programs and initiatives. These types of engagements foster broad public sector partner involvement in actively developing CIKR protection priorities and requirements. Through the SLTTGCC Annual Report, the Council provides annual updates on CIKR programs and initiatives that are being conducted or planned by the Council, DHS, other Federal partners, or private sector partners.

7.1.4 Regional Consortium Coordinating Council Reporting to DHS

Cross-sector and multi-jurisdictional CIKR protection challenges provide an opportunity to manage interdependent risks at the regional level. Individually, the activities of the regional consortium enhance the physical security, cybersecurity, emergency preparedness, and overall public-private continuity and resiliency of one or more States, urban areas, or municipalities. The RCCC provides a unique mechanism to integrate NIPP implementation on a regional scale and details its efforts in the RCCC Annual Report.

7.1.5 Aggregating Submissions to DHS

DHS uses the information collected from the Sector CIKR Protection Annual Reports, the SLTTGCC Annual Report, the RCCC Annual Report, and State reports to assess CIKR protection status and requirements across the country. As national priorities and requirements are established, DHS will develop funding recommendations for programs and initiatives designed to reduce national-level risk in the CIKR protection mission area. In cases where gaps or duplicative efforts exist, DHS will work with the SSAs and the States to identify strategies or additional funding sources to help ensure that national CIKR protection priorities are efficiently and effectively addressed.

Following the collection, aggregation, and risk-based analysis of sector- and State-level reports, DHS summarizes this information in the National CIKR Protection Annual Report. This report details national CIKR protection priorities and requirements, and makes recommendations for prioritized focus across the Federal Government to meet national-level CIKR protection needs. The National CIKR Protection Annual Report is submitted along with the DHS budget submission to the EOP on or before September 1 as part of the annual Federal budget process (see figure 7-1).

Figure 7-1: National CIKR Protection Annual Report Process

7.2 Federal Resource Prioritization for DHS, the SSAs, and Other Federal Agencies

The Federal prioritization process described in this section is designed to ensure that the collective efforts of DHS, the SSAs, and other Federal departments and agencies support the NIPP and national priorities. It is also designed to be consistent with the DHS responsibility to coordinate overall national CIKR protection and identify national-level gaps, overlaps, or shortfalls. Driven in large part by existing and well-understood Federal budget process milestones, this approach is integrated into the established Federal budget process and reporting requirements. The process outlined in this chapter recognizes the existing budget authority and responsibilities of all Federal departments and agencies with CIKR protection-related programs and activities. We have achieved significant progress in developing a comprehensive CIKR risk management program. We will continually improve our risk management and performance measurement programs to refine their integration into the Federal budget process. The NIPP process aims to create synergy between current and future efforts to ensure a unified and effective national CIKR protection effort. The specific roles of DHS and the SSAs are described in further detail below.

7.2.1 Department of Homeland Security

DHS is responsible for overall coordination of the Nation's CIKR protection efforts. To carry out this responsibility, DHS must: identify and prioritize nationally critical assets, systems, networks, and functions; help ensure that appropriate protective initiatives are implemented; and help address any gaps or shortfalls in the protection of nationally critical CIKR. DHS works closely with the EOP to aggregate CIKR protection-related activities and related resource requests from the SSAs, other Federal departments and agencies, and other CIKR partners as a way to make informed tradeoffs in prioritizing Federal investments. These tradeoffs also consider other CIKR protection requirements that the various Federal departments and agencies must address.

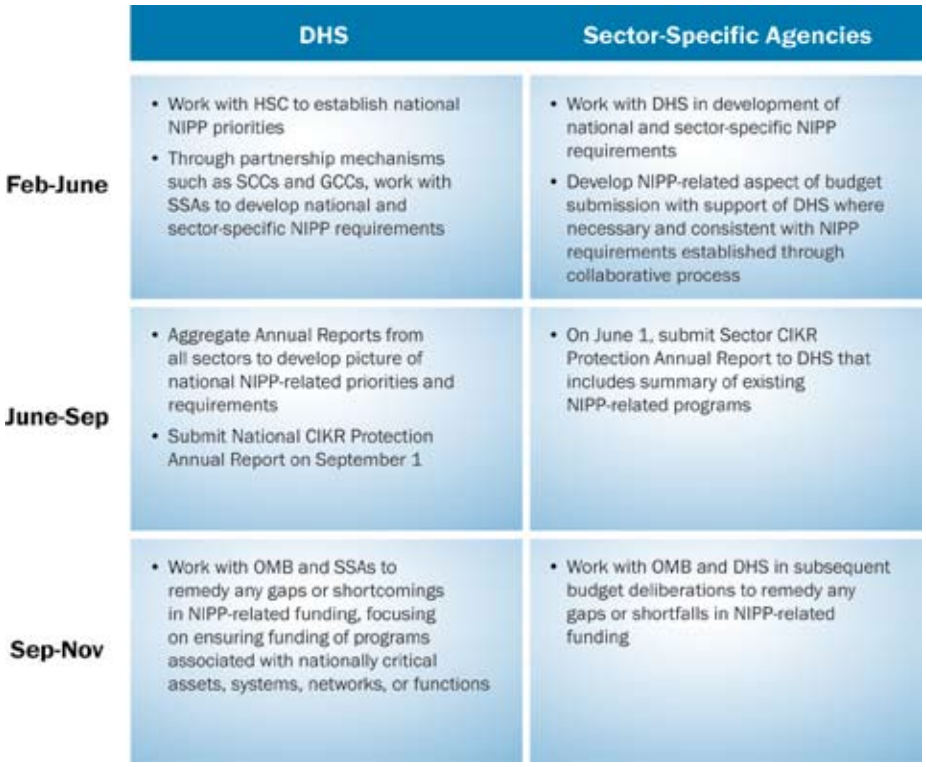
DHS works with the EOP to establish a national CIKR protection strategic approach and priorities, and with the SSAs, supported by their respective SCCs and GCCs, to develop sector-specific CIKR protection-related requirements. Driven largely by the identification and prioritization of critical assets, systems, networks, and functions across sectors and States, the establishment of national protection priorities helps inform resource allocation decisions later in the process. The SSAs communicate information about their existing CIKR protection-related programs and outstanding requirements to DHS through their Sector CIKR Protection Annual Reports. DHS uses the sector annual reports, as well as the annual reports of the SLTTGCC and the RCCC, to inform the National CIKR Protection Annual Report. The National CIKR Protection Annual Report analyzes information about sector priorities, requirements, and programs in the context of the National Risk Profile, a high-level summary of the aggregate risk and protective status of all sectors. The National Risk Profile drives the development of national priorities, which, in turn, are used to assess existing CIKR programs and to identify existing gaps or shortfalls in national CIKR protection efforts. This analysis provides the Executive Office of the President with information that supports both strategic and investment decisions related to CIKR protection and resiliency.

Figure 7-2: National CIKR Protection Annual Report Analysis

7.2.2 Sector-Specific Agencies

Earlier chapters of the NIPP articulated how DHS and the SSAs work with the respective CIKR sectors to determine risk and set priorities. Based on guidance from DHS, each SSA develops and maintains an SSP that supports the NIPP; some SSPs may also fulfill other mandates and requirements. Additionally, the SSAs, in partnership with the SCCs and GCCs, determine sector-specific priorities and requirements for CIKR protection. The SSAs submit these priorities and requirements to DHS in their sector annual reports. The SSAs work within their respective department or agency budget process to determine the CIKR protection-related aspects of their department's budget submission. SSA annual reports are submitted to DHS on or before June 1 of each year. Resource information contained in the SSA annual reports is based on appropriated funding, as well as the President's most recent budget.

Figure 7-3: DHS and SSA Roles and Responsibilities in Federal Resource Allocation



Additionally, the subset of CIKR protection funding requirements directed toward R&D and S&T investments are highlighted by the SSAs, SCCs, and GCCs in the sector 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 are based on the R&D planning section of each sector's SSP. The identified R&D requirements are prioritized based on the potential increase in CIKR protection capabilities for a given investment.

7.2.3 Summary of Roles and Responsibilities

Figure 7-3 outlines the roles and responsibilities of DHS and the SSAs throughout this process, as well as the annual timelines associated with major activities.

The final determination of funding priorities, based on the collaborative efforts of DHS, the SSAs and other Federal departments and agencies, and the EOP, guides CIKR protection programs in support of the NIPP and other applicable requirements. These priorities support Federal Government (DHS and SSA) CIKR protection activities, as well as guide and support homeland security and CIKR protection activities across and within State, local, tribal, and territorial jurisdictions.

7.3 Federal Resources for State and Local Government Preparedness

Federal grants from DHS and other Federal agencies, when available, and other programs, such as training and technical assistance, offer key support to State and local jurisdictions for CIKR protection programs. These programs provide resources to meet CIKR needs that are managed by State and local entities.

GPD 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. GPD offers State, local, and tribal partners access to funding through several grant programs that can be leveraged to support CIKR protection requirements based on risk and need.

For the purposes of the NIPP, Federal grants available through DHS/GPD can be grouped into two broad categories: (1) overarching homeland security 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 Guidelines; and (2) targeted infrastructure protection programs for specific CIKR-related protection initiatives and programs within identified jurisdictions. States should 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 vulnerabilities and close identified capability gaps related to CIKR within their jurisdictions.

7.3.1 Overarching Homeland Security Grant Programs

The overarching homeland security grant programs support activities that are conducted in accordance with the National Preparedness Guidelines. These funds support overall State and local homeland security efforts, and can be leveraged to support State, local, tribal, and/or regional CIKR protection. These funds are intended to complement and be allocated in coordination with national CIKR protection efforts.

The primary overarching homeland security grant programs include:

- **State Homeland Security Program (SHSP)**: The SHSP supports the implementation of the State Homeland Security Strategy to address identified planning, organizing, equipment, training, exercise, and evaluation needs for acts of terrorism. In addition, SHSP supports the implementation of the National Preparedness Guidelines, the NIMS, the NRF, and the NIPP to support the prevention of, protection against, response to, and recovery from acts of terrorism.
- **Urban Areas Security Initiative**: UASI funds address the unique planning, organizing, equipment, training, exercise, and evaluation 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.

7.3.2 Targeted Infrastructure Protection Programs

Targeted infrastructure protection programs include grants for specific activities that focus on the protection of CIKR, such as ports, mass transit, rail transportation, etc. These funds support CIKR protection capabilities based on risk and need in coordination with DHS, SSAs, and Federal agencies.

IP and GPD work with States to focus targeted infrastructure protection grant programs, such as the BZPP and transportation security grants, to support national-level CIKR protection priorities and to reinforce activities funded through Federal department and agency budgets and other homeland security grant programs. As appropriate, SSAs serve as subject matter experts reviewing and providing recommendations for specific target grant programs. Grantees should apply resources available under the overarching homeland security grant programs, such as SHSP and UASI, to address their regionally or locally critical CIKR protection initiatives. An additional prioritized combination of grant funding across various programs may be necessary to enable the protection of certain assets, systems, networks, and functions deemed to be nationally critical.

Available GPD grant funding is awarded to the Governor-appointed State administrative agency, which serves in each State as the lead for program implementation. Through the State administrative agencies, States will identify and prioritize their homeland security needs, including CIKR protection, and leverage assistance from these funding streams to accomplish 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 Guidelines; the National Priorities, including implementation of the NIPP; and capabilities enhancements based on the TCL.

DHS provides State, local, and tribal authorities with additional guidance on how to identify, assess, and prioritize CIKR protection needs and programs in support of the National Preparedness Guidelines as they apply to homeland security grants. Additional information on DHS grant programs, guidelines, allocations, and eligibility is available at: http://www.fema.gov/grants.

7.4 Other Federal Grant Programs That Contribute to CIKR Protection

Other Federal departments and agencies provide grant programs that can contribute to CIKR protection. These are usually sector- or threat-specific programs; many are related to technology development initiatives. Examples of these grant programs include:

- **Department of Energy**: DOE manages programs for the development of technologies to increase the resilience and reliability of the U.S. energy infrastructure. These programs address the development and demonstration of technologies and methodologies to protect physical energy infrastructure assets.
- **Department of the Interior**: The Bureau of Indian Affairs manages a grant program for the Safety of Dams on Indian Lands. Financial awards are specific to a given site; awards are restricted to Indian tribes or tribal organizations.
- **Department of Justice**: The National Institute of Justice (NIJ), Office of Justice Programs, manages a grant program for Domestic Anti-Terrorism Technology Development. The objective of the program is to support the development of counterterrorism technologies, assist in the development of standards for those technologies, and work with State and local jurisdictions to identify particular areas of vulnerability to terrorist acts and to be better prepared to respond if such acts occur. The NIJ is authorized to make grants to, or enter into contracts or cooperative agreements with, State and local governments, private nonprofit organizations, public nonprofit organizations, for-profit organizations, institutions of higher education, and qualified individuals. Applicants from the Territories of the United States and federally recognized Indian tribal governments are also eligible to participate in this program.

- **Department of Transportation**: The Pipeline and Hazardous Materials Safety Administration Pipeline Safety grant program supports efforts to develop and maintain State natural gas, liquefied natural gas, and hazardous liquid pipeline safety programs. Grant recipients are typically State government agencies.
- **Department of Transportation**: The Federal Transit Administration is a grants-in-aid agency that has several major assistance programs for eligible activities. Funds are provided through legislative formulas or discretionary authority. Funding from these programs is provided on an 80/20 Federal/local funding match basis unless otherwise specified. These assistance programs can contribute to CIKR protection efforts through funding for metropolitan and State planning and research grants; urban, non-urban, and rural transit assistance programs; bus and railway modernization efforts; major capital investments; and special flexible-funding programs.

These programs are available to a wide range of grant recipients, including CIKR owners and operators, and State, local, and tribal governments.

7.5 Setting an Agenda in Collaboration with CIKR Protection Partners

Resource allocation decisions for CIKR 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 government and private sector partners to set the national agenda that specifies this strategic approach to CIKR protection, articulates associated requirements, supports collaboration among partners, and recognizes the contributions of private sector partners to the overall effort. While Federal Government funding of programs and initiatives that support CIKR 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 effective use of Federal and non-Federal resources.

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

These opportunities for collaboration allow private sector owners and operators to benefit from CIKR protection investments in a number of ways. First, investments in CIKR protection will enable risk mitigation in a broader, all-hazards context, including common threats posed by malicious individuals or acts of nature, in addition to those posed by terrorist organizations. Second, business continuity planning can facilitate recovery of commercial activity after an incident. Finally, investing in CIKR protection within the NIPP framework will help private sector owners and operators enhance protective measures, and will support decisionmaking with more comprehensive risk-informed information. DHS explores new opportunities to encourage such collaboration through incentives (such as the SAFETY Act, which creates liability protection for sellers of qualified anti-terrorism technologies), and by providing useful information on risk assessment and management. While States typically are the eligible applicants for DHS grant programs, certain private sector entities can apply directly for grant funds through programs such as the Port Security Grant Program and the Intercity Bus Security Grant Program.

More information about the NIPP is available on the Internet at: www.dhs.gov/nipp or by contacting DHS at: nipp@dhs.gov

List of Acronyms and Abbreviations

BZPP	Buffer Zone Protection Program
C/ACAMS	Constellation/Automated Critical Asset Management System
CAEIAE	Centers of Academic Excellence in Information Assurance Education
CEO	Chief Executive Officer
CFATS	Chemical Facility Anti-Terrorism Standards
CFDI	Critical Foreign Dependencies Initiative
CFIUS	Committee on Foreign Investment in the United States
CFR	Code of Federal Regulations
CII	Critical Infrastructure Information
CIKR	Critical Infrastructure and Key Resources
CIPAC	Critical Infrastructure Partnership Advisory Council
CWIN	Critical Infrastructure Warning Information Network
COG	Continuity of Government
COI	Community of Interest
COOP	Continuity of Operations
COP	Common Operating Picture
CSIA IWG	Cyber Security and Information Assurance Interagency Working Group
CSIRT	Computer Security Incident Response Teams
DHS	Department of Homeland Security
DoD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOT	Department of Transportation
ECTF	Electronic Crimes Task Force
E.O.	Executive Order
EOP	Executive Office of the President
EPA	Environmental Protection Agency
FACA	Federal Advisory Committee Act
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEMA	Department of Homeland Security/Federal Emergency Management Agency
FIRST	Forum of Incident Response and Security Teams
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FSLC	Federal Senior Leadership Council
GCC	Government Coordinating Council
GFIRST	Government Forum of Incident Response and Security Teams
GPD	FEMA/Grant Programs Directorate (Division of DHS Preparedness Directorate)
GPS	Global Positioning System
GSA	General Services Administration
HHS	Department of Health and Human Services
HITRAC	Department of Homeland Security's Homeland Infrastructure Threat and Risk Analysis Center
HMGP	Hazard Mitigation Grant Program
HSAC	Homeland Security Advisory Council
HSAS	Homeland Security Advisory System
HSC	Homeland Security Council
HSEEP	Homeland Security Exercise and Evaluation Program
HSIN	Homeland Security Information Network
HSIN-CS	Homeland Security Information Network for Critical Sectors
HSIP	Homeland Security Infrastructure Program
HSOC	Homeland Security Operations Center
HSPD	Homeland Security Presidential Directive
iCAV	Integrated Common Analytical Viewer

IDW	Infrastructure Data Warehouse
IED	Improvised Explosive Device
IICD	Infrastructure Information Collection Division
IICP	Infrastructure Information Collection Program
IICS	Infrastructure Information Collection System
IICV	Infrastructure Information Collection and Visualization
IDM	Infrastructure Data Management
IP	Office of Infrastructure Protection (Division of DHS National Protection and Programs Directorate)
IRAPP	Infrastructure Risk Analysis Partnership Program
ISAC	Information Sharing and Analysis Center
ISE	Information-Sharing Environment
IWWN	International Watch and Warning Network
IV	Infrastructure Visualization
JCG	Joint Contact Group
JTTF	Joint Terrorism Task Force
LEO	Law Enforcement Online
MIFC	Maritime Intelligence Fusion Center
MS-ISAC	Multi-State Information Sharing and Analysis Center
NATO	North Atlantic Treaty Organization
NCC	National Coordinating Center for Telecommunications
NCIP R&D	National Critical Infrastructure Protection Research and Development
NCRCG	National Cyber Response Coordination Group
NCS	National Communications System
NCSA	National Cyber Security Alliance
NCSD	DHS National Cyber Security Division
NCTC	National Counterterrorism Center
NEP	National Exercise Program
NHC	National Hurricane Center
NIAC	National Infrastructure Advisory Council
NIAP	National Information Assurance Partnership
NICC	National Infrastructure Coordinating Center
NIJ	National Institute of Justice
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NISAC	National Infrastructure Simulation and Analysis Center
NIST	National Institute of Standards and Technology
NJTTF	National Joint Terrorism Task Force
NOC	National Operations Center
NOC-HQE	National Operations Center—Headquarters Element
NRC	Nuclear Regulatory Commission
NRCC	National Response Coordination Center
NRF	National Response Framework
NSA	National Security Agency
NSC	National Security Council
NS/EP	National Security and Emergency Preparedness
NSTAC	National Security Telecommunications Advisory Committee
NSTC	National Science and Technology Council
OAS	Organization of American States
OCA	Original Classification Authority
OECD	Organisation for Economic Co-operation and Development
OI&A	Office of Intelligence and Analysis (Division of DHS Preparedness Directorate)
OMB	Office of Management and Budget
OSTP	Office of Science and Technology Policy
PCC	Policy Coordination Committee
PCII	Protected Critical Infrastructure Information
PDD	Presidential Decision Directive
PNT	Position, Navigation, and Timing
PSA	Protective Security Advisor
PVTSAC	Private Sector Senior Advisory Committee
RCCC	Regional Consortium Coordinating Council
R&D	Research and Development
RISS	Regional Information Sharing Systems

SAV	Site Assistance Visit
SCADA	Supervisory Control and Data Acquisition
SCC	Sector Coordinating Council
SHIRA	Strategic Homeland Infrastructure Risk Analysis
SHSP	State Homeland Security Program
SLFC	State and Local Fusion Center
SLTTGCC	State, Local, Tribal, and Territorial Government Coordinating Council
SPP	Security and Prosperity Partnership of North America
SSA	Sector-Specific Agency
SSI	Sensitive Security Information
SSP	Sector-Specific Plan
S&T	Science and Technology Directorate of DHS
SVA	Security Vulnerability Assessment
TCL	Target Capabilities List
TSA	Transportation Security Administration
UASI	Urban Areas Security Initiative
UCNI	Unclassified Controlled Nuclear Information
UDOP	User Defined Operational Picture
U.S.	United States
U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team
USCG	United States Coast Guard
UTL	Universal Task List
VBIED	Vehicle Borne Improvised Explosive Device
ViSAT	Vulnerability Identification Self-Assessment Tool
WMD	Weapons of Mass Destruction

Glossary of Key Terms

Many of the definitions in this Glossary are derived from language enacted in Federal laws and/or included in national plans, including the Homeland Security Act of 2002, the USA PATRIOT Act of 2001, the National Incident Management System, and the National Response Framework. Additional definitions come from the DHS Lexicon.

All-Hazards. A grouping classification encompassing all conditions, environmental or manmade, that have the potential to cause injury, illness, or death; damage to or loss of equipment, infrastructure services, or property; or alternatively causing functional degradation to social, economic, or environmental aspects.

Asset. Person, structure, facility, information, material, or process that has value. In the context of the NIPP, people are not considered assets.

Business Continuity. The ability of an organization to continue to function before, during, and after a disaster.

Chemical Facility Anti-Terrorism Standards (CFATS). Section 550 of the DHS Appropriations Act of 2007 grants the Department of Homeland Security the authority to regulate chemical facilities that "present high levels of security risk." The CFATS establish a risk-informed approach to screening and securing chemical facilities determined by DHS to be "high risk."

CIKR Partner. Those Federal, State, local, tribal, or territorial governmental entities, public and private sector owners and operators and representative organizations, regional organizations and coalitions, academic and professional entities, and certain not-for-profit and private volunteer organizations that share in the responsibility for protecting the Nation's CIKR.

Consequence. The effect of an event, incident, or occurrence. For the purposes of the NIPP, consequences are divided into four main categories: public health and safety, economic, psychological, and governance impacts.

Control Systems. Computer-based systems used within many infrastructure 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 SCADA systems, Process Control Systems, and Distributed Control Systems.

Critical Infrastructure. Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction.

Critical Infrastructure Information (CII). Information that is not customarily in the public domain and is related to the security of critical infrastructure or protected systems. CII consists of records and information concerning any of the following:

- Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law; harms the interstate commerce of the United States; or threatens public health or safety.
- The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit.
- Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, insurance, or continuity, to the extent that it is related to such interference, compromise, or incapacitation.

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 confidentiality, integrity, and availability. Includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems.

Cyber System. Any combination of facilities, equipment, personnel, procedures, and communications integrated to provides cyber services. Examples include business systems, control systems, and access control systems.

Dependency. The one-directional reliance of an asset, system, network, or collection thereof, within or across sectors, on input, interaction, or other requirement from other sources in order to function properly.

Function. Service, process, capability, or operation performed by an asset, system, network, or organization.

Government Coordinating Council. The government counterpart to the SCC for each sector established to enable interagency coordination. The GCC comprises representatives across various levels of government (Federal, State, local, tribal, and territorial) as appropriate to the security and operational landscape of each individual sector.

Hazard. Natural or manmade source or cause of harm or difficulty.

HSPD-19. This directive establishes a national policy and calls for the development of a national strategy and implementation plan on the prevention and detection of, protection against, and response to terrorist use of explosives in the United States.

Incident. An occurrence, caused by either human action or natural phenomena, that may cause harm and may require action. Incidents can include major disasters, emergencies, terrorist attacks, terrorist threats, wild and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, and other occurrences requiring an emergency response.

Infrastructure. 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 in the Homeland Security Act, infrastructure includes physical, cyber, and/or human elements.

Interdependency. Mutually reliant relationship between entities (objects, individuals, or groups). The degree of interdependency does not need to be equal in both directions.

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

Mitigation. Ongoing and sustained action to reduce the probability of or lessen the impact of an adverse incident.

Network. A group of components that share information or interact with each other in order to perform a function.

Normalize. In the context of the NIPP, the process of transforming risk-related data into comparable units.

Owners/Operators. Those entities responsible for day-to-day operation and investment in a particular asset or system.

Preparedness. Activities necessary to build, sustain, and improve readiness capabilities to prevent, protect against, respond to, and recover from natural or manmade incidents. Preparedness is a continuous process involving efforts at all levels of government and between government and the private sector and nongovernmental organizations to identify threats, determine vulnerabilities, and identify required resources to prevent, respond to, and recover from major incidents.

Prevention. Actions taken and measures put in place for the continual assessment and readiness of necessary actions to reduce the risk of threats and vulnerabilities, to intervene and stop an occurrence, or to mitigate effects.

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

Protected Critical Infrastructure Information (PCII). PCII refers to all critical infrastructure information, including categorical inclusion PCII, that has undergone the validation process and that the PCII Program Office has determined qualifies for protection under the CII Act. All information submitted to the PCII Program Office or Designee with an express statement is presumed to be PCII until the PCII Program Office determines otherwise.

Protection. Actions or measures taken to cover or shield from exposure, injury, or destruction. In the context of the NIPP, protection includes actions to deter the threat, mitigate the vulnerabilities, or minimize the consequences associated with a terrorist attack or other incident. Protection can include a wide range of activities, such as hardening facilities, building resiliency and redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing security systems, promoting

workforce surety, training and exercises, and implementing cybersecurity measures, among various others.

Recovery. The development, coordination, and execution of service- and site-restoration plans for affected communities and the reconstitution of government operations and services through individual, private sector, nongovernmental, 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.

Resilience. The ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions.

Response. Activities that address the short-term, direct effects of an incident, including 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; increasing 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. The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.

Risk-Informed Decisionmaking. The determination of a course of action predicated on the assessment of risk, the expected impact of that course of action on that risk, and other relevant factors.

Risk Management Framework. A planning methodology that outlines the process for setting goals and objectives; identifying assets, systems, and networks; assessing risks; prioritizing and implementing protection programs and resiliency strategies; measuring performance; and taking corrective action. Public and private sector entities often include risk management frameworks in their business continuity plans.

Sector. A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society. The NIPP addresses 18 CIKR sectors, identified by the criteria set forth in HSPD-7.

Sector Coordinating Council. The private sector counterpart to the GCC, these councils are self-organized, self-run, and self-governed organizations that are representative of a spectrum of key stakeholders within a sector. SCCs serve as the government's principal point of entry into each sector for developing and coordinating a wide range of CIKR protection activities and issues.

Sector Partnership Model. The framework used to promote and facilitate sector and cross-sector planning, coordination, collaboration, and information sharing for CIKR protection involving all levels of government and private sector entities.

Sector Specialists. DHS Sector Specialists provide coordination and integration capability across the CIKR sectors to provide senior DHS decisionmakers with strategic (national-level) situational awareness and assessments of CIKR impacts both on a steady-state basis and during incidents.

Sector-Specific Agency. Federal departments and agencies identified in HSPD-7 as responsible for CIKR protection activities in specified CIKR sectors.

Sector-Specific Plan. Augmenting plans that complement and extend the NIPP Base Plan and detail the application of the NIPP framework specific to each CIKR sector. SSPs are developed by the SSAs in close collaboration with other sector partners.

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. Any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose.

Terrorism. Premeditated threat or act of violence against noncombatant persons, property, and environmental or economic targets to induce fear, intimidate, coerce, or affect a government, the civilian population, or any segment thereof, in furtherance of political, social, ideological, or religious objectives.

Threat. A natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.

Tier 1. Tier 1 facilities and systems are those that if successfully destroyed or disrupted through terrorist attack would cause major national or regional impacts similar to those

experienced with Hurricane Katrina or the September 11, 2001, attacks.

Tier 2. Tier 2 facilities and systems are those that meet predefined, sector-specific criteria and that are not Tier 1 facilities or systems.

Value Proposition. A statement that outlines the national and homeland security interest in protecting the Nation's CIKR and articulates the benefits gained by all CIKR partners through the risk management framework and public-private partnership described in the NIPP.

Vulnerability. A physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.

Weapons of Mass Destruction. Weapon capable of a high order of destruction and/or of being used in such a manner as to destroy large numbers of people or an amount of property.

Appendix 1: Special Considerations

Appendix 1A: Cross-Sector Cybersecurity

1A.1 Introduction

The United States relies on cyber infrastructure for government operations, a vibrant economy, and the health and safety of its citizens. However, malicious actors can and do conduct attacks against critical cyber infrastructure on an ongoing basis. While both public and private sector owners and operators actively manage the risk to their operations through monitoring and mitigation activities designed to prevent daily incidents from becoming significant disruptions, increasingly sophisticated threats require a more thorough examination of cyber risk and the associated risks to cybersecurity. Furthermore, nation-states are realizing that hacking tools, methods, and tactics offer asymmetric opportunities for espionage, countering military force, and economic and geopolitical advantages. These threat vectors, combined with insider threat and a range of other pervasive cyber threats to critical infrastructure, highlight the need for public, private, academic, and international entities to collaborate and enhance cybersecurity awareness and preparedness efforts, and to ensure that the cyber elements of CIKR are:

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

While Chapter 3 of the NIPP discusses specific cybersecurity concerns during each phase of the NIPP risk management framework, the following sections of this appendix discuss the processes, procedures, tools, programs, and methodologies that public and private sector entities, CIKR sectors, academic institutions, and international entities can use to enhance cybersecurity.

1A.1.1 Value Proposition for Cybersecurity

The value proposition for cybersecurity aligns with that for CIKR protection in general, as discussed in chapter 1 of the NIPP, but with a concentrated focus on cyber infrastructure. Many CIKR functions and services are enabled through cyber systems

and services; if cybersecurity is not appropriately addressed, the risk to CIKR is increased. The responsibility for cybersecurity spans all CIKR partners, including public and private sector entities. The NIPP provides a coordinated and collaborative approach to help public and private sector partners understand and manage cyber risk.

The NIPP promotes cybersecurity by facilitating participation and partnership in CIKR protection initiatives, leveraging cyber-specific expertise and experiences, and improving information exchange and awareness of cybersecurity concerns. It also provides a framework for public and private sector partner efforts to recognize and address the similarities and differences among the approaches to cyber risk management for business continuity and national security. This framework enables CIKR partners to work collaboratively to make informed cyber risk management decisions, define national cyber priorities, and address cybersecurity as part of an overall national CIKR protection strategy.

1A.1.2 Definitions

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

- **Cyber Infrastructure**: Includes electronic information and communications systems and services and the information contained therein. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information. For example: computer systems; control systems (e.g., SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) are part of cyber infrastructure:
  - Producers and providers of cyber infrastructure and services represent the information technology industrial base and make up the Information Technology Sector. The producers and providers of cyber infrastructure and services play a key role in developing secure and reliable products and services.
  - Consumers of cyber infrastructure must maintain its security as new vulnerabilities are identified and the threat environment evolves. 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 CIKR.
- **Information Technology (IT)**: These critical functions are sets of processes that produce, provide, and maintain products and services. IT critical functions encompass the full set of processes (e.g., R&D, manufacturing, distribution, upgrades, and maintenance) involved in transforming supply inputs to IT products and services.
- **Cybersecurity**: The prevention of damage to, unauthorized use of, exploitation of, and, if needed, the restoration of electronic information and communications systems and services (and the information contained therein) to ensure confidentiality, integrity, and availability.
- **Cross-Sector Cybersecurity**: Collaborative efforts among DHS, the SSAs, and other CIKR partners to improve the cybersecurity of the CIKR sectors by facilitating cyber risk-mitigation activities.

1A.1.3 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 four primary authorities associated with cybersecurity are the National Strategy to Secure Cyberspace, HSPD-7, NSPD-54/HSPD-23, and the Homeland Security Act. These documents are described in further detail in appendix 2A.

1A.2 Cybersecurity Responsibilities

The National Strategy to Secure Cyberspace, HSPD-7, NSPD-54/HSPD-23, and the Homeland Security Act identify the responsibilities of the various CIKR 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 HSPD-7, DHS is a principal focal point for the security of cyberspace. DHS has specific responsibilities regarding the coordination of the efforts of CIKR partners to prevent damage, unauthorized use, and exploitation and to enable the restoration of cyber infrastructure to ensure confidentiality, integrity, and availability. These responsibilities include:

- Developing a comprehensive national plan for securing U.S. CIKR;
- Providing crisis management in response to incidents involving cyber infrastructure;
- Providing technical assistance to other governmental entities and the private sector with respect to emergency recovery plans for incidents involving cyber infrastructure;
- Coordinating with other Federal agencies to provide specific warning information and advice on appropriate protective measures and countermeasures to: State, local, and tribal governments; the private sector; academia; and the public;
- Conducting and funding cybersecurity R&D, in partnership with other agencies, which will lead to new scientific understanding and technologies in support of homeland security; and
- Assisting the 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 CIKR;
- Promoting a comprehensive national awareness program to empower businesses, the workforce, and individuals to secure their own segments of cyberspace;
- Working with CIKR partners to reduce cyber vulnerabilities and minimize the severity of cyber attacks;
- Coordinating the development and conduct of national cyber threat assessments;
- Providing input on cyber-related issues for the National Intelligence Estimate of cyber threats to the United States;
- Facilitating cross-sector cyber analysis to understand and mitigate cyber risk;
- Providing guidance, review, and functional advice on the development of effective cyber-protective measures; and
- Coordinating cybersecurity programs and contingency plans, including the recovery of Internet functions.

1A.2.2 Sector-Specific Agencies

Recognizing that each CIKR sector possesses its own unique characteristics and operating models, the SSAs provide subject matter and industry expertise through relationships with the private sector to enable protection of the assets, systems, networks, and functions that they provide within each of the sectors. The SSAs are working with their private sector counterparts to understand and mitigate cyber risk by:

- Identifying subject matter expertise regarding 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 CIKR inventory, risk assessment, and protective measures currently: address cyber assets, systems, and networks; require enhancement; or require the 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, as appropriate;
- Establishing planning, training, and exercise programs according to HSEEP; and

- Exchanging cyber-specific information with sector 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 cyber infrastructure while maintaining an awareness of vulnerabilities and consequences to ensure that the cyber infrastructure is not used to enable attacks against the Nation's CIKR. 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 the 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 or mitigate cyber threats by acquiring more robust data on victims of cyber crime and intrusions;
  - Leading the national effort to investigate and prosecute those who conduct or attempt to conduct cyber attacks;
  - Exploring the means to provide sufficient investigative and forensic resources and training to facilitate expeditious investigation and resolution of CIKR incidents; and
  - Identifying ways to improve cyber information sharing and investigative coordination among Federal, State, local, and tribal law enforcement communities; other agencies; and the private sector.
- **The Federal Bureau of Investigation and the Intelligence Community**: Ensuring a strong counterintelligence posture to deter intelligence collection against the Federal 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 threats or attacks to enable a timely and effective response.

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

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

- Managing the security of their cyber infrastructure while maintaining an awareness of threats, vulnerabilities, and consequences to ensure that it is not used to enable attacks against CIKR, and ensuring that 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 cyber infrastructure appropriately;
- Establishing planning, training, and exercise programs according to HSEEP; and
- Establishing cybersecurity programs, including policies, plans, procedures, recognized business practices, awareness, and audits.

1A.2.5 Owners and Operators

Owners and operators are encouraged to implement the following recommendations as indicated in the National Strategy to Secure Cyberspace:

- Managing the security and resiliency of their cyber infrastructure while maintaining an awareness of vulnerabilities and consequences to ensure that it is not used to enable attacks against the Nation's CIKR;
- Participating in sector-wide programs to share information on cybersecurity;
- Evaluating the security of networks that affect the security of the Nation's CIKR, including:

  - Conducting audits to ensure effectiveness and the use of best practices;
  - Developing continuity plans that consider the full spectrum of necessary resources, including off-site staff and equipment; and
  - Participating in industry-wide information sharing and best practices dissemination;
- Reviewing and exercising continuity plans for cyber infrastructure and examining alternatives (e.g., diversity in service providers, implementation of recognized cybersecurity practices) as a way of improving resiliency and mitigating risk;
- Identifying near-term R&D priorities that include programs for highly secure and trustworthy hardware, software, and protocols; and
- Promoting more secure out-of-the-box installation and implementation of software industry products, including: increasing user awareness of the security features of 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 cyber infrastructure while maintaining awareness of vulnerabilities and consequences to ensure that it is not used to enable attacks against the Nation's CIKR;
- 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 Cross-Sector Cybersecurity Programs

Since each sector has a unique reliance on cyber infrastructure, DHS will assist the SSAs in developing a range of effective and appropriate cyber-protective measures. To assist the SSAs, DHS has established several vulnerability-reduction programs under the NIPP risk management framework, including:

- **Critical Infrastructure Protection Cybersecurity (CIP CS) Program**: The CIP CS Program strengthens preparedness by partnering with the public and private sectors to improve the security of the IT Sector and cybersecurity across the Nation's critical infrastructure by facilitating risk management activities that reduce cyber vulnerabilities and minimize the severity of cyber attacks. The program includes responsibility for the development and implementation of the IT SSP; for cross-sector cyber support to SSAs as they maintain and implement their SSPs and reduce cyber risk to their sectors; and support to IP for development of the NIPP's cyber component, SSP development guidance and technical assistance sessions, and the National CIKR Protection Annual Report.
- **Software Assurance Program**: Public and private sector 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 effort that addresses people,

Cyber Security Vulnerability Assessment (CSVA)

Developed by the DHS National Cyber Security Division (NCSD) CIP CS Program, the CSVA is a flexible and scalable approach that analyzes an entity's cybersecurity posture and describes gaps and targeted considerations that can reduce overall cyber risks.

The CSVA assesses the policies, plans, and procedures in place to reduce cyber vulnerabilities and leverages various recognized standards, guidance, and methodologies (e.g., International Organization for Standardization 27001, Information Systems Audit and Control Association (ISACA) Control Objects for Information and Related Technologies (COBIT), and the NIST Special Publication 800 series).

processes, technology, and acquisition throughout the software life cycle. Focused on shifting away from the current security paradigm of patch management, these efforts will encourage the production of higher quality, more secure software. These efforts to promote a broader ability to routinely develop and deploy trustworthy software products through public-private partnerships are a significant element of securing cyberspace and the Nation's CIKR. DHS also partners with NIST in the National Information Assurance Partnership (NIAP), a Federal Government initiative originated to meet the security testing needs of both information technology consumers and producers. NIAP is operated by NSA to address security testing, evaluation, and validation programs.

- **Control System Security Program**: The NCSD Control System Security Program coordinates efforts among Federal, State, local, tribal, and territorial governments, as well as control system owners, operators, and vendors to improve control system security within and across all CIKR sectors. The Control System Security Program coordinates activities to reduce the likelihood of the success and severity of a cyber attack against critical infrastructure control systems through risk-mitigation activities. These activities include assessing and managing control system vulnerabilities, assisting the US-CERT Control Systems Security Center with control system incident management, and providing control system situational awareness through outreach and training initiatives.

Control System Cyber Security Self-Assessment Tool (CS2SAT)

Developed by the NCSD Control System Security Program, the CS2SAT is a desktop software tool that guides users through a step-by-step process to assess their control system network and then makes appropriate recommendations for improving the system's cybersecurity posture based on recognized security standards.

The tool derives its recommendations from a database of cybersecurity practices that have been adapted specifically for application to industry control system networks and components.

Each recommendation is linked to a set of actions that can be applied to remediate specific security vulnerabilities.

- **The Standards and Best Practices Program**: As part of its efforts to develop practical guidance and review tools, and to promote R&D investment in cybersecurity, DHS and NIST co-sponsor the National Vulnerability Database. This database provides centralized and comprehensive vulnerability mitigation resources for all types of users, including the general public, system administrators, and vendors to assist with incident prevention and management (including links to patches) to mitigate consequences and vulnerabilities.
- **The Cyber Exercise Program**: Through this program, DHS and CIKR partners conduct exercises to improve coordination among members of the cyber incident response community, including Federal, State, local, tribal, territorial, and international governmental entities, as well as private sector corporations, coordinating councils, and academic institutions. The main objectives of national cyber exercises are to: practice coordinated response to cyber attack scenarios; provide an environment for evaluation of interagency and cross-sector processes, procedures, and tools for communications and response to cyber incidents; and foster improved information sharing among government agencies and between government and private industry.

In addition to specific DHS cybersecurity infrastructure protection programs, DHS has partnered with other public and private sector entities to develop and implement specific programs to help improve the security of cyber infrastructure across sectors, as well as to support national cyber risk-mitigation activities, including:

- **Government Forum of Incident Response and Security Teams (GFIRST)**: Following the model of the global FIRST organization, the Federal interagency community established 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 who are responsible for securing government IT systems. The members work together to understand and deal with computer security incidents and to encourage proactive and preventive security practices.
- **Cross-Sector Cybersecurity Working Group (CSCSWG)**: The CSCSWG serves as a forum to bring government and the private sector together to collaboratively address risk across the CIKR sectors. This cross-sector perspective facilitates the sharing of perspectives and knowledge about various cybersecurity concerns, such as common vulnerabilities and protective measures, and leverages functional cyber expertise in a comprehensive forum.
- **The National Cyber Response Coordination Group (NCRCG)**: The NCRCG 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 crisis. NCRCG member agencies use their established relationships with the private sector and State,

local, tribal, and territorial governments to facilitate cyber incident management, develop courses of action, and devise appropriate response and recovery strategies. NCRCG facilitates coordination of the Federal Government's efforts to prepare for, respond to, and recover from cyber incidents and physical attacks that have significant cyber consequences.

The Federal Government is continually increasing their capability to address cyber risk associated with critical networks and information systems beyond the previously mentioned DHS and DHS-partnered programs and entities. NSPD-54/HSPD-23 outlined the Comprehensive National Cybersecurity Initiative (CNCI) and a series of continuous efforts designed to establish a frontline defense by: reducing current vulnerabilities and preventing intrusions; defending against the full spectrum of threats by using intelligence and strengthening supply chain security; and shaping the future environment by enhancing our research, development, and education, as well as investing in leap-ahead technologies.

NSPD-54/HSPD-23 directs the Secretary of Homeland Security, in consultation with the heads of other SSAs, to submit a report detailing the policy and resource requirements for improving the protection of privately owned U.S. CIKR networks. The report details how the Federal Government can partner with the private sector to leverage investment in technology, increase awareness about the extent and severity of the cyber threats facing CIKR, and enhance real-time cyber situational awareness. Under the auspices of the CIPAC, DHS formed a private sector CIKR working group to respond to this task. Private sector input proved to be critical in enabling DHS to fully appreciate the scale and scope of the task and to develop a set of actionable recommendations that accurately reflect the reality of the shared responsibility between the public and private sectors with respect to securing the Nation's cyber assets, systems, and networks. DHS is now working through the CIPAC and NIPP Partnership Framework to implement the short- and long-term recommendations in the report, as well as engage the private sector in other CNCI activities.

1A.4 Ensuring Long-Term Cybersecurity

The effort to ensure a coherent cyber CIKR 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 protection of cyber assets, systems, and networks, and the functions that they provide, 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 the 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, territorial, and private sector 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 CIKR 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 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:

- FBI's Cyber Task Forces involve more than 50 law enforcement agency cyber task forces and more than 80 additional cyber working groups throughout the country, collaborating with Federal, State, and local partners to maximize investigative resources to ensure a timely and effective response to cybersecurity threats of both a criminal and a national security nature.
- FBI's InfraGard program is a public-private partnership coordinated out of the 56 FBI field offices nationwide. This 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 Crimes Task Forces provide interagency coordination on cyber-based attacks and intrusions.

Information Sharing and Analysis Centers: Underscoring the effectiveness of cybersecurity efforts is the importance of information sharing between and among industry and government. To this end, the Information Technology and Communications ISACs work closely together and with DHS and the SSAs to maximize resources, coordinate preparedness and response efforts, and maintain situational awareness to enable risk mitigation regarding cyber infrastructure.

Cybersecurity Awareness for CIKR Partners: DHS plays an important 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), including 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.
- Engaging with the MS-ISAC to help enhance the Nation's cybersecurity readiness and response at the State and local levels, and launching a national cybersecurity awareness effort in partnership with the MS-ISAC. The MS-ISAC is an information-sharing organization, with representatives of State and local governments, that analyzes, sanitizes, and disseminates information pertaining to cyber events and vulnerabilities to its constituents and private industry.
- Collaborating with the NCSA, the MS-ISAC, and the public and private sector to establish October as National Cyber Security Awareness Month and participating in activities to continuously raise cybersecurity awareness nationwide.

Cyberspace Emergency Readiness: DHS established the US-CERT, which is a 24/7 single point of contact for cyberspace analysis and 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 that is designed to help secure the Nation's Internet infrastructure and coordinate defenses against and responses to cyber attacks across the Nation. US-CERT is responsible for:

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

To support the information-sharing requirements of the network approach, US-CERT provides the following information on their Web site, which is accessible through the HSIN and by mail:

- **Cybersecurity Alerts**: Written in a language for home, corporate, and new users, these alerts are published in conjunction with technical alerts in the context of security issues that affect the general public.
- **Cybersecurity Bulletins**: Bulletins summarize information that has been published regarding emergent security issues and vulnerabilities. They are published weekly and are written primarily for systems administrators and other technical users.
- **Cybersecurity Tips**: Tips provide information and advice on a variety of common cybersecurity topics. They are published biweekly and are written primarily for home, corporate, and new users.
- **National Web Cast Initiative**: In an effort to increase cybersecurity awareness and education among the States, DHS, through US-CERT and the MS-ISAC, has launched a joint partnership to develop a series of national Web casts that will examine critical and timely cybersecurity issues. The purpose of this initiative is to strengthen the Nation's cyber readiness and resilience.
- **Technical Cybersecurity Alerts**: Written for systems administrators and experienced users, technical alerts provide timely information on current cybersecurity issues and vulnerabilities.

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

1A.4.2 International Coordination on Cybersecurity

The Federal Government proactively uses its intelligence capabilities to protect the country from cyber attack, its diplomatic outreach and operational capabilities to build partnerships in the global community, and its law enforcement capabilities to combat cyber crime wherever it originates. The private sector, international industry associations, and companies with global interests and operations are also engaged in addressing cybersecurity internationally. For example, the U.S.-based Information Technology Association of America participates in international cybersecurity conferences and forums, such as the India-based National Association for Software and Service Companies Joint Conference. These efforts involve interaction with both the policy and operational communities to coordinate national and international activities that are mutually supportive around the globe:

- **International Cybersecurity Outreach**: DHS, in conjunction with the DOS and other Federal agencies, engages in multilateral and bilateral discussions to further international security awareness and policy development, as well as incident response team information-sharing and capacity-building objectives. The United States engages in bilateral discussions on important cybersecurity issues with close allies and others with whom the United States shares networked interdependencies, to include, but not limited to, Australia, Canada, Egypt, Germany, Hungary, India, Italy, Japan, the Netherlands, Romania, the United Kingdom, etc. The United States also provides leadership in multilateral and regional forums addressing cybersecurity and CIKR protection to encourage all nations to take systematic steps to secure their networked systems. For example, U.S. initiatives include the APEC Telecommunications Working Group capacity-building program to help member countries develop CSIRTs and the OAS framework proposal to create a regional computer incident response point-of-contact network for information sharing and to help member countries develop CSIRTs. Other U.S. efforts to build a culture of cybersecurity include participation in OECD, G8, and United Nations activities. The U.S. private sector is actively involved in this international outreach in partnership with the Federal Government.
- **Collaboration on Cyber Crime**: The U.S. outreach strategy for comprehensive cyber laws and procedures draws on the Council of Europe Convention on Cyber Crime, as well as on the following: (1) the G8 High-Tech Crime Working Group's principles for fighting cyber crime and protecting critical information infrastructure; (2) the OECD guidelines on information and network security; and (3) the United Nations General Assembly resolutions based on the G8 and OECD efforts. The goal of this outreach strategy is to encourage individual nations and regional groupings of nations to join DHS in its efforts to protect internationally interconnected national systems.
- **Collaborative Efforts for Cyber Watch, Warning, and Incident Response**: The Federal Government is working strategically with key allies on cybersecurity policy and operational cooperation. For example, DHS is leveraging pre-existing relationships among CSIRTs. DHS also has established a preliminary framework for cooperation on cybersecurity policy, watch, warning, and incident response with key allies. The framework also incorporates efforts related to key strategic issues as agreed on by these allies. An IWWN is being established among cybersecurity policy, computer emergency response, and law enforcement participants representing 15 countries. The IWWN will provide a mechanism through which the participating countries can share information in order to build global cyber situational awareness and coordinate incident response.
- **Partnerships to Address the Cyber Aspects of Critical Infrastructure Protection**: DHS and the SSAs are leveraging existing agreements, such as the SPP and the JCG with the United Kingdom, to address the IT Sector and cross-cutting cyber components of CIKR protection. The trilateral SPP builds on existing bilateral agreements between the United States and Canada and the United States and Mexico by allowing issues to be addressed on a dual binational basis. In the context of the JCG, DHS established a 10-point action plan to address cybersecurity policy, watch, warning, incident response, and other strategic 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 in the future.

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

- DHS developed the IT Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development. The EBK characterizes the IT security workforce and provides a national baseline representing the essential knowledge and skills that IT security practitioners should have to perform specific roles and responsibilities. Specifically, the EBK does the following:
  - Articulates the functions that professionals within the IT security workforce perform in a context-neutral format and language;
  - Promotes uniform competency guidelines to increase the overall efficiency of IT security education, training, and professional development; and
  - Provides content guidelines that can be leveraged to facilitate cost-effective professional development of the IT workforce, including future skills training and certification, academic curricula, or other affiliated human resources activities.
- DHS co-sponsors the National CAEIAE program with NSA. There are now 94 centers of academic excellence across 38 States. Together, DHS and NSA are working to expand the program to more universities.
- DHS collaborates with the National Science Foundation to co-sponsor and expand the Federal Cyber Services: Scholarship for Service Program. The Scholarship for Service Program provides grant money to selected CAEIAE universities to fund the final 2 years of 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. Agents from ICE, the Internal Revenue Service, and the U.S. Secret Service attended the basic 6½-week course. This training was funded through the Treasury Executive Office of Asset Forfeiture.
- Through DHS, DOJ, DoD, and DOS, the Federal Government provides cyber-related training to foreign cyber incident responders (incident response management, creation of CSIRTs) and law enforcement personnel and jurists (law, computer forensics, case handling).

1A.4.4 Research and Development

The Cyber Security Research and Development Act of 2002 authorized a multi-year 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's OSTP established a Cyber Security and Information Assurance Interagency Working Group (CSIA IWG) under the NSTC. The CSIA IWG was jointly chartered by NSTC's Subcommittee on Networking and Information Technology R&D and the Subcommittee on Infrastructure. This interagency working group includes participants from 20 organizations representing 11 departments and agencies, as well as several offices in the White House.

The purpose of the working group is to coordinate Federal programs for cybersecurity and information assurance R&D. It also is responsible for developing the Federal Plan for Cyber Security and Information Assurance R&D, which includes near-term, mid-term, and long-term cybersecurity research efforts in response to the National Strategy to Secure Cyberspace and HSPD-7. The document includes descriptions of approximately 50 cybersecurity R&D topics, such as: Automated Attack Detection, Warning, and Response; Forensics, Traceback, and Attribution; Security Technology and Policy Management Methods; Policy Specification Languages; and Integrated, Enterprise-Wide Security Monitoring and Management. The document also identifies the top cybersecurity and information assurance research topics across the Federal Government. Finally, the document includes key findings and recommendations. DHS actively co-chairs the CSIA IWG with OSTP and continues to identify critical cyber R&D requirements for incorporation into Federal R&D planning efforts.

1A.4.5 Exploring Private Sector Incentives

Awareness and understanding of the need for cybersecurity present a challenge for both government and industry. Although cybersecurity requires significant investments in time and resources, an effective cybersecurity program may reduce the likelihood of a successful cyber attack or reduce the impact if a cyber attack occurs. Network disruptions resulting from cyber attacks

can lead to loss of money, time, products, reputation, sensitive information, or even potential loss of life through cascading effects on critical systems and infrastructure. From an economic perspective, cyber attacks have resulted in billions of dollars of business losses and damages in the aggregate.

The private sector makes risk management decisions, including those for cybersecurity, based on the return on investment and the desire to ensure business continuity. Market-based incentives for cybersecurity investments include protection of intellectual capital, security-influenced procurement, market differentiation, and public confidence. Sometimes, however, cyber assets, systems, or networks may be deemed to be nationally critical and necessitate additional risk management beyond that which the private sector implements as part of their corporate responsibility. To address this difference, the CSCSWG is examining an array of possible incentives for increased investment in cybersecurity.

Appendix 1B: International CIKR Protection

1B.1 Introduction and Purpose of This Appendix

This appendix provides guidance for addressing the international aspects of CIKR protection in support of the NIPP.

1B.1.1 Scope

The NIPP provides the mechanisms, processes, key initiatives, and milestones necessary to enable DHS, DOS, SSAs, and other partners—both foreign and domestic—to strengthen international cooperation to protect U.S. CIKR, both at home and abroad. The NIPP and associated SSPs recognize that protective measures do not stop at a facility's fence or at a national border. Because disruptions in global infrastructure can have ripple effects around the world, the NIPP and the SSPs also consider cross-border CIKR, international vulnerabilities, and global 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 coordinated, comprehensive, and aggressive global action as a key aspect of the NIPP approach to CIKR protection.

This approach involves identifying those CIKR that, if damaged or destroyed, are capable of causing national or regional catastrophic effects on security, public safety, or the economy. HSPD-7 and the 9/11 Commission Act of 2007 support the NIPP mandate to identify the Nation's critical foreign dependencies so that appropriate risk management strategies may be developed. Furthermore, the National Strategy to Secure Cyberspace sets forth strategic objectives for maintaining national security and ensuring international cooperation on cybersecurity, including preventing cyber attacks against America's critical infrastructure, reducing vulnerabilities, and building resiliency into systems and networks in order to minimize the damage and recovery time from any cyber attacks and incidents that occur.

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

The NIPP strategy for international coordination in CIKR protection outlined in this appendix is focused on effective cooperation with international partners rather than on specific protective measures. Specific measures are tailored to each sector's particular circumstances and are described in the SSPs and addressed as part of the CFDI (see section 4.1.4.1). This appendix also discusses existing international agreements that affect CIKR protection and addresses cross-sector and global issues such as the Nation's critical foreign dependencies and cybersecurity.

DHS, DOS, and other concerned Federal departments and agencies work together on an ongoing basis to ensure that the NIPP strategy for international coordination on CIKR protection remains current and is incorporated into the strategies of all Federal partners, as appropriate, to provide a consistent framework for cooperating with other countries and international/multinational organizations. This effort focuses on: promoting a global culture of physical security and cybersecurity; managing CIKR-related risk beyond the physical borders of the United States; accelerating international cooperation in order to develop intellectual infrastructure based on shared assumptions and compatible conceptual tools; and connecting constituencies not traditionally engaged in CIKR protection. The broad structure of this approach is based on the following high-level considerations.

1B.2 Responsibilities for International Cooperation on CIKR Protection

In accordance with HSPD-7, DOS, in conjunction with DHS, DOJ, DoD, the Departments of Commerce and Treasury, the NRC, and other appropriate departments and agencies, is responsible for working with foreign countries and international/multinational organizations to strengthen the protection of U.S. CIKR. This section describes the responsibilities of various partners for ensuring and promoting international cooperation in CIKR protection.

1B.2.1 Department of Homeland Security

Under the NIPP risk management framework described in chapter 3, DHS, in collaboration with DOS and other CIKR partners, is responsible for the following actions, all of which have an international dimension:

- Identifying and prioritizing the Nation's critical foreign dependencies through the CFDI;
- Building and strengthening international partnerships;
- Implementing a comprehensive, integrated international CIKR risk management program;
- Implementing protective programs and resiliency strategies; and
- Sharing appropriate information with international entities and performing outreach functions to enhance information exchange and management of international agreements on CIKR protection.

Some of the more complex challenges presented by the international aspects of CIKR protection involve analyzing the complex dependencies, interdependencies, and vulnerabilities that require the application of sophisticated and innovative modeling techniques. DHS is responsible for pursuing research and analysis in this area and will call on a range of outside sources for this work, including those with expertise in the international community and the 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 and has the overarching lead for U.S. foreign relations, policies, and activities, as well as for the advancement of U.S. interests abroad. The Secretary of State, in conjunction with the Secretary of Homeland Security and specific SSAs, as appropriate, is responsible for coordinating with foreign countries and international organizations to strengthen the protection of critical foreign dependencies. DOS supports the efforts of DHS and other Federal partners by providing knowledge of and access to foreign governments and leveraging bilateral and multilateral relationships around the world to promote the importance of CIKR protection and the priority CIKR, as defined through CFDI. In this way, DOS also supports the sharing of best practices related to CIKR protection to ensure that the Federal Government can act effectively to identify and protect U.S. CIKR.

1B.2.3 Other Federal Departments and Agencies

SSAs exchange information, as appropriate, including cyber-specific information, with CIKR partners in other countries. These information-sharing activities are conducted in accordance with guidelines established by DHS and DOS and other Federal departments/agencies to improve the Nation's overall CIKR protection posture.

Under HSPD-7, Federal departments and agencies share the responsibility for working through DOS to reach out to foreign countries and international organizations to strengthen CIKR protection. Federal departments and agencies also have the responsibility for identifying, prioritizing, and managing the risks associated with the Nation's critical foreign dependencies, as well as identifying and prioritizing CIKR located overseas through the CFDI.

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

DHS works with State, local, tribal, and territorial governments to help ensure ongoing cooperation with relevant CIKR protection efforts within their jurisdictions and geographic areas. State and local governments, in coordination with DOS and DHS, may also have a cross-border role in regions where there are existing cross-border associations and emergency response agreements.

1B.2.5 Private Sector

DHS works with the private sector and nongovernmental organizations to protect cross-border infrastructure and understand critical foreign dependencies, as well as international and global vulnerabilities. DHS relies on the private sector for data, expertise, and knowledge of their international operations to identify critical international assets, systems, and networks, and assess global risks, including shared threats and interdependencies. DHS uses such information to inform the National Critical Foreign Dependencies List and associated risk management activities.

1B.2.6 Academia

The academic community provides data, insight, and research into the significance of international interdependencies through modeling, simulation, and analysis.

1B.3 Managing the International Dimension of CIKR Risk

The NIPP addresses international CIKR protection, including interdependencies and the vulnerability to threats that originate outside the country. The NIPP brings a new focus to international cooperation and provides a risk-informed strategic framework for measuring the effectiveness of international CIKR 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 supports collaborative engagement with additional international partners.

The SSPs include international considerations as an integral part of each sector's planning process. Some international aspects of CIKR protection require additional overarching or cross-sector emphasis. These include:

- U.S. interactions with foreign governments and international organizations to enhance the confidentiality, integrity, and availability of cyber-based infrastructure, which often has an international or even global dimension;
- Protection of physical assets located on, near, or extending across the borders with Canada and Mexico, or those with important economic supply chain implications that require cooperation with and/or planning and resource allocation among neighboring countries, States bordering these countries, and affected local and tribal governments and the private sector;
- Sectors with CIKR that are extensively integrated into an international or global market (e.g., Banking and Finance or other information-based sectors, Energy, or Transportation Systems), or sectors whose proper functioning relies on input originating from outside the United States; and
- U.S. Government and corporate facilities located overseas (e.g., protection for the Government Facilities Sector involves careful interagency collaboration, as well as cooperation with foreign CIKR partners).

The following subsections discuss issues associated with the international aspects of CIKR protection in the context of the steps of the NIPP risk management framework (see chapter 3).

1B.3.1 Setting Goals and Objectives

The overarching goal of the NIPP—to enhance the protection of U.S. CIKR—applies to the international "system of systems" that underpins U.S. CIKR. The NIPP and the SSPs provide guidance and risk management approaches to address the international aspects of CIKR protection efforts on both a national and a sector-specific level. In addition, a separate set of goals and priorities guides cross-sector and global efforts to improve protection for CIKR with international linkages. These goals fall into three categories:

- Identifying, prioritizing, and addressing cross-sector and global issues;
- Implementing existing and developing new agreements that affect CIKR; and
- Improving the effectiveness of international cooperation.

DHS, in conjunction with DOS and other CIKR partners, defines the requirement for a comprehensive international CIKR protection strategy. The integration of international CIKR protection considerations and measures into each SSP supports the pursuit and achievement of 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.

1B.3.2 Identifying CIKR Affected by International Linkages or Located Internationally

Once international CIKR protection goals and objectives are set, the next step in the risk management process is to develop and maintain a comprehensive inventory of the Nation's CIKR located outside U.S. borders and of foreign CIKR, the damage or destruction of which may lead to loss of life in the United States or critically affect the Nation's public health, economy, or national and homeland security capabilities. The process for identifying these CIKR involves working with U.S. industry, SSAs, academia, and international partners to gather and protect information on the foreign infrastructure and resources on which the United States relies or which significantly affect U.S. interests as noted above. This process has been formalized through the CFDI, and results in a prioritized list of assets and systems critical to effectively managing international risks in the CIKR protection mission area.

The NIPP risk management framework details a structured approach for determining dependencies and interdependencies, including physical, cyber, and international considerations. This approach is designed to address CIKR protection needs and vulnerabilities in three areas:

- Direct international linkages to U.S. physical, human, and cyber CIKR:
  - Foreign cross-border assets linked to U.S. CIKR (e.g., roads, bridges, rail lines, pipelines, gas lines, telecommunications lines and undersea cables and facilities, and power lines physically connecting U.S. CIKR to Canada and Mexico);
  - Foreign infrastructure, the disruption or destruction of which could directly harm the U.S. homeland (e.g., a Canadian dam that could flood U.S. territory, a Mexican chemical plant that could affect U.S. territory, or foreign ports and facilities where security failures could directly affect U.S. security); and
  - U.S. CIKR that is located overseas (e.g., non-military government facilities or overseas components of U.S. CIKR).
- Indirect international linkages to physical, human, and cyber U.S. CIKR:
  - The potential cascading and escalating effects of disruptions to foreign assets, systems, and networks such as critical foreign technology, goods and services, resources, transit routes, and chokepoints; and
  - Foreign ownership, control, or involvement in U.S. CIKR and related issues.
- Global aspects of physical and cyber U.S. CIKR:

– Assets, systems, and networks located around the world or with global mobility that require the efforts of multiple foreign countries to effectively manage the associated risks to CIKR.

Analysis of the dependencies and interdependencies is based primarily on information from each sector and the input of CIKR owners and operators regarding their supply chains and sources of services from other infrastructure sectors (e.g., Energy and Water). As the capability for sophisticated network analysis grows, these inputs are complemented by assessments that examine less apparent dependencies and interdependencies. The NISAC supports this effort by analyzing national and international dependencies and interdependencies for complex systems and networks.

1B.3.3 Assessing Risks

Risk assessment for CIKR 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 are summarized in the following three-step process that applies equally to CIKR with international linkages:

- Determine the consequences of destruction, incapacitation, or exploitation of CIKR. This is done to assess the potential national significance, as well as physical, cyber, and human dependencies and interdependencies that may result from international linkages.
- Analyze vulnerabilities, including determining which elements of CIKR are most susceptible to attack or disruption (this includes analyzing whether particular international linkages increase the attractiveness of these elements as a target of an attack).
- Conduct a threat analysis to identify the likelihood that a target will be attacked. CIKR with international linkages may present greater opportunities for attack.

Issues important to other countries may differ from those of primary importance to the United States. Risk analysis needs to be conducted in coordination with other countries to draw on their perspectives and expertise, as well as our own.

1B.3.4 Prioritizing CIKR

Assessing CIKR 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, natural disasters, and other emergencies. The HITRAC, through the CFDI and the NISAC, and in coordination with DOS and other public and private sector partners, is responsible for developing the Nation's prioritized list of critical foreign dependencies. Such prioritization helps to inform national goals, foreign engagement, and allows the NIPP community to pursue a coordinated strategy for CIKR risk management. The CFDI is described in greater detail below.

In accordance with the NIPP, the Federal Government created an initial inventory of infrastructure located outside the United States that if disrupted or destroyed would lead to loss of life in the United States or critically affect the Nation's economy or national security. Using this inventory as a starting point, DHS worked with DOS to develop the CFDI, a process designed to ensure that the resulting classified list of critical foreign dependencies is representative and leveraged in a coordinated and inclusive manner.

- **Phase I—Identification (annual)**: DHS, working with other Federal partners, developed the first-ever National Critical Foreign Dependencies List in FY2008, reflecting the critical foreign dependencies of the CIKR sectors, as well as critical foreign dependencies of interest to the Nation as a whole. The identification process includes input from public and private sector CIKR community partners.
- **Phase II—Prioritization (annual)**: DHS, in collaboration with other CIKR community partners and, in particular, DOS, prioritized the National Critical Foreign Dependencies List based on factors such as the overall criticality of the CIKR to the United States and the willingness and capability of foreign partners to engage in collaborative risk management activities.
- **Phase III—Engagement (ongoing)**: Phase III involves leveraging the prioritized list to guide current and future U.S. bilateral and multilateral incident and risk management activities with foreign partners. DHS and DOS established mechanisms to ensure coordinated engagement and collaboration by public entities, in partnership with the private sector.

1B.3.5 Implementing Programs

The SSAs, in collaboration with other CIKR partners, are responsible for developing protective measures to address risks arising from international factors that affect CIKR within their sectors. 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 international CIKR protection:

- **International Outreach Program**: DHS works with DOS and other Federal departments and agencies with foreign affairs responsibilities to conduct international outreach with foreign countries and international organizations to encourage the promotion and adoption of organizational 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 infrastructure on which the United States depends. These efforts reflect the prioritization of international CIKR and serve as an extension of the CFDI's engagement phase.
- **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 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 response and recovery efforts during a cyber incident. The NCRCG consults with international partners for routine situational awareness and during incidents. NCRCG member agencies integrate their capabilities to facilitate assessment of the domestic and international scope and severity of a cyber incident.
- **National Exercise Program (NEP)**: DHS provides overarching coordination for the NEP 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 NEP provides opportunities through exercises for international partners to engage with Federal, State, and local departments and agencies to address cooperation and cross-border issues, including those related to CIKR protection. DHS and other CIKR partners also participate in exercises sponsored by international partners, including cross-border, multi-sector tabletop exercises.
- **National Cyber Exercises**: DHS conducts exercises to identify, test, and improve the coordination of the cyber incident response community, including Federal, State, local, tribal, territorial, and international governmental entities, as well as private sector corporations and coordinating councils.

Because of the complex nature of the international dimension of CIKR, a substantial emphasis is placed on best practices that can be used to improve cooperation and coordination. To this end, DHS leads efforts to:

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

1B.3.6 Measuring Effectiveness and Making Improvements

Metrics are used to manage the comprehensive international CIKR protection strategy outlined in the NIPP and to track progress toward the strategy's three goals:

- Improving the effectiveness of international cooperation;
- Implementing existing and developing new agreements that affect CIKR; and
- Addressing cross-sector and global CIKR protection issues.

DHS, in cooperation with other Federal departments and agencies, develops data and metrics to track progress on international CIKR protection activities. These data and metrics include:

- The international issues faced by each sector that affect multiple sectors and the relative importance of these issues;
- The countries that should be involved in protection partnerships for each sector;
- The number and type of bilateral and multinational agreements that affect CIKR protection;
- The nature, extent, 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 CIKR protection enhancements that directly result from a particular international initiative.

1B.4 Organizing International CIKR Protection Cooperation

DHS, in conjunction with DOS and other Federal departments and agencies, works with individual foreign governments, as well as regional and international organizations, to enhance CIKR protection on an international basis and to deny opportunities for exploitation of CIKR assets. Potential partnerships depend on:

- Physical proximity to the United States or U.S. CIKR;
- Useful experience and information to be gained from other countries;
- Existing relationships, alliances, agreements, and high-level commitments; and
- Critical supply chains and vulnerable nodes.

As international CIKR protection partnerships mature, cooperative efforts strengthen in two dimensions:

- Development of new partnerships with countries possessing useful experience and information regarding CIKR protection efforts, as well as terrorism prevention, preparedness, response, and recovery; and
- Development of new international relationships and frameworks to protect global infrastructure and address international interdependencies, networked technologies, and the need for a global culture of physical security and cybersecurity.

The coordination mechanisms supporting the NIPP create linkages between CIKR protection efforts at the national, sector, State, local, tribal, territorial, regional, and international levels. A diverse group of entities is involved with this coordination, based on the specific issues that they address, as well as other considerations, as discussed in this section.

1B.4.1 U.S. and Foreign Government Activities and Interactions

DHS works with domestic and international CIKR partners to exchange experiences and information, and to develop a cooperative relationship that will result in material improvement in U.S. CIKR protection, information sharing, cybersecurity, and global telecommunications standards. Through efforts such as the CFDI, DHS, DOS, and other Federal partners work with specific countries to identify international interdependencies and vulnerabilities. The SSAs address international factors such as cross-border infrastructure, international vulnerabilities, and global interdependencies in their SSPs.

The International Affairs offices in Federal departments and agencies maintain relationships with their counterpart foreign ministries and agencies, and play a principal role with DOS in coordinating with foreign governments on international CIKR matters.

International cooperation on issues such as cybersecurity and energy supply is necessary because of the global nature of these types of infrastructure. Such efforts require interaction on both the policy and operational levels and involve a broad range of entities from both government and the private sector. To address cybersecurity, DHS established a framework for cooperation on cybersecurity policy, watch and warning, and incident response for CIKR with key allies such as Australia, Canada, New Zealand, and the United Kingdom. DHS is coordinating and participating in the establishment of an IWWN among policy,

computer emergency response, and law enforcement participants in 15 countries. The IWWN provides an information-sharing mechanism through which participating countries can build cyber situational awareness and coordinate incident response.

DHS, SSAs, and other U.S. partners work with other countries to promote CIKR protection best practices and pursue infrastructure security through international/multilateral organizations such as the Group of Eight (G8), NATO, European Union, OAS, OSCE, OECD, and Asia-Pacific Economic Cooperation (APEC). International cooperation on CIKR protection takes place bilaterally, regionally, and multilaterally. The approach to working with some specific countries and organizations is founded on formal agreements that address cooperation on CIKR protection, as described below.

- **Canada and Mexico**: The CIKR of the United States and its immediate neighbors are closely interconnected and cover a wide range of sectors. Electricity, natural gas, oil, telecommunications, roads, rail, food, water, minerals, and finished products cross the borders on a regular basis as part of normal commerce. The importance of this trade, and the infrastructure that supports it, was highlighted after the terrorist attacks of September 11, 2001, nearly closed both borders. The United States entered into the 2001 Smart Border Accord with Canada and the 2002 Border Partnership Plan with Mexico, in part, to address bilateral CIKR issues. In addition, the 2005 SPP established a trilateral approach to common security issues. The SPP complements existing agreements.
- **United Kingdom**: The United Kingdom is a close ally of the United States who has much experience in fighting terrorism and protecting its CIKR. The United Kingdom has developed substantial expertise in law enforcement and intelligence systems, and in the protection of commercial facilities based on its counterterrorism experience. Like the United States, most of the critical infrastructure in the United Kingdom is privately owned. The government of the United Kingdom developed an effective, sophisticated system to manage public-private partnerships. DHS formed a JCG with the United Kingdom that brings officials into regular, formal contact to discuss and resolve a range of bilateral homeland security issues.
- **The Group of Eight (G8)**: Since September 11, 2001, the infrastructure in several G8 countries has been exploited and used to inflict casualties and fear. As a result, G8 partners underscored their determination to combat all forms of terrorism and to strengthen international cooperation. To that end, within the G8 context, the United States spearheaded various critical infrastructure protection initiatives in 2007 and 2008. The first project focused on G8 delegation nation security planning best practices, vulnerability assessment methodologies, and threat assessments for critical energy infrastructure. The second project focused on chemical sector infrastructure protection activities, which was a timely subject given the release of the CFATS in the United States during the previous year. These projects have increased the baseline understanding of the measures underway, as well as the CIKR protection capabilities of each G8 member nation. The G8 offers an effective forum through which members can work to reduce global risks to CIKR by sharing best practices and methodologies, and understanding common threats. Future projects related to critical infrastructure protection within the G8 will address issues related to interdependencies within and across infrastructure systems.
- **European Union**: The United States is engaged in a number of CIKR protection and resiliency activities with the European Union, including those related to advising the European Union on CIKR risk analysis and management, writ large, as well as counter-explosive device activities. The European Commission is in the process of implementing the EPCIP. This program will affect all 27 nations in the European Union, as well as potentially others in the Euro-Zone that elect to participate. EPCIP will initially focus on the energy and transport sectors, with expanded focus on the telecommunications, financial, and chemical sectors in coming years. The United States has engaged the EPCIP leadership for the purpose of offering the assistance necessary to support the implementation of the program, with the ultimate goal of enhancing CIKR protection activities wherever they may be found. Furthermore, IP and S&T work with the DOS Bureau of Diplomatic Security's Office of Antiterrorism Assistance and the Office of the Coordinator for Counterterrorism, DOJ, and FBI to coordinate with the European Union to conduct workshops, seminars, and exercises on countering terrorist use of explosive devices.
- **North Atlantic Treaty Organization (NATO)**: NATO addresses CIKR issues through the Senior Civil Emergency Planning Committee, the senior policy and advisory body to the North Atlantic Council on civil emergency planning and disaster relief matters. The committee is responsible for policy direction and coordination of Planning Boards and Committees in the NATO environment. It has developed considerable expertise that applies to CIKR protection and has implemented planning boards and committees covering ocean shipping, inland surface transport, civil aviation, food and agriculture, industrial prepared-

ness, civil communications planning, civil protection, and civil-military medical issues. DHS: provides a delegation to the Senior Civil Emergency Planning Committee at NATO; participates in NATO's telecommunications working group and the critical infrastructure protection coordination group; has expert NATO representation on the Civil Protection Committee and Industrial Planning Committee; and engages with NATO in preparedness exercises.

1B.4.2 Foreign Investment in U.S. CIKR

CIKR protection may be affected by foreign investment and ownership of sector assets. At the Federal level, this issue is monitored by the CFIUS. The committee is chaired by the Secretary of the Treasury, with membership that includes: the Secretaries of State, Defense, Commerce, and Homeland Security; the Attorney General; the Directors of the OMB and the OSTP; the U.S. Trade Representative; the Chairman of the Council of Economic Advisors; the Assistant to the President for Economic Policy; and the Assistant to the President for National Security Affairs. The CFIUS is the Federal inter-agency body charged with addressing potential conflicts between maintaining open U.S. markets and ensuring national and homeland security.

As a member of CFIUS, DHS examines the potential impact of proposed foreign investments on current and planned CIKR protection activities. The committee develops and negotiates security agreements with foreign entities to manage any CIKR risks that foreign investment may pose. DHS leads government monitoring activities to ensure compliance with these agreements.

DHS also partners with DOJ and other Federal departments and agencies to review applications to the FCC from foreign entities pursuant to section 214 of the Communications Act of 1934. DHS supports these reviews to assess whether the proposed activities pose any threat to CIKR protection.

1B.4.3 Information Sharing

Effective international cooperation on CIKR protection requires information-sharing systems that include processes and protocols for real-time information sharing and communication of threats and relevant intelligence reports. Successful international cooperation also requires mechanisms for the systematic sharing of best practices and frequent opportunities for partners to meet in order to discuss international CIKR issues.

The NOC serves as the Nation's hub for information sharing and situational awareness for domestic incident management and is responsible for increasing coordination (through the NICC) among those members of the international community who are involved because of the role that they play in enabling the protection of U.S. CIKR.

The HSIN supports ongoing information-sharing efforts by offering COIs for selected international partners requiring close coordination with the NICC and NOC.

DHS also provides mechanisms (e.g., the US-CERT portal) to improve information sharing and coordination among government communities and selected international partners for cybersecurity. The Cybercop portal is a secure, Internet-based information-sharing mechanism for law enforcement personnel involved in electronic crimes investigation. This collaborative tool links the law enforcement community worldwide, supporting participants from more than 40 countries.

1B.5 Ensuring International Cooperation Over the Long Term

Ensuring a sustainable approach to the international aspects of CIKR protection over the long term requires special consideration in the following areas:

- **Awareness**: Awareness of international aspects of CIKR protection issues helps ensure implementation of effective, coordinated, and integrated CIKR protection measures and enables CIKR partners to make informed decisions. Often, these issues are not apparent to those who can take the most effective action because of the complexity of the international systems affecting CIKR protection. Awareness programs designed to identify and address such issues are required to ensure continued international support for protection programs over the long term. DHS is collaborating with DOS and other NIPP partners to build awareness of the international aspects of CIKR protection and their importance in developing effective protective programs and resiliency strategies in this global age.

- **Training and Education**: NIPP training courses for the managers and staff responsible for CIKR should cover international considerations for CIKR protection because of the complex issues that often accompany international linkages and initiatives. DHS ensures that the organizational and sector expertise needed to implement the international aspects of the NIPP program over the long term are developed and maintained through exercises and other mechanisms that promote international cooperation on CIKR protection. For example, IP, S&T, DOS, and DOJ work with the European Union to conduct workshops, seminars, and exercises on methods and technologies for countering explosive devices.
- **Research and Development**: Cooperative and coordinated R&D efforts are one of the most effective ways to improve protective capabilities or dramatically lower the costs of existing capabilities so that international CIKR partners can afford to do more with limited resources. Techniques and designs developed through research can cost very little to share with international CIKR partners and, although the lead times needed for maturation of technology from the laboratory to the field can be decades, such improvements can have wider applicability or much greater effectiveness than available through current methods. Several Federal departments and agencies monitor international R&D efforts to avoid duplication and identify projects that may affect U.S. Government interests and activities. For example, S&T's International Programs Division evaluates international R&D projects that S&T may leverage to benefit U.S. homeland security and CIKR protection efforts. DHS, DoD, DOE, and DOJ all collaborate with international partners, as does the interagency TSWG, to develop technological solutions to defeat terrorism threats, including threats to CIKR.
- **Vulnerability Assessments**: Over the past several years, DHS has worked with U.S. interagency partners in DOS, DOE, and the U.S. Army Corps of Engineers, among others, to conduct vulnerability assessments on international CIKR of interest to the United States. These assessments have included essential bridges and tunnels at the northern border with Canada, critical dams at the southern border with Mexico, locks and levees in Panama, and Energy Sector installations in a Caribbean nation. The purpose of these assessments is to protect U.S. interests abroad and to provide assistance, training, and other support to U.S. allies and partners. As the critical infrastructure protection capabilities within the United States continue to mature, more nations will seek assistance and expertise from the United States and the United States will continue to identify CIKR assets of interest on foreign or shared soil. Opportunities to increase the global CIKR protection posture should be undertaken where appropriate.
- **Plan Updates**: Annual reviews and updates of the NIPP and SSPs must consider the current international situation and be coordinated, as appropriate, with international agreements affecting CIKR protection. As the SSPs are reviewed for reissue in 2010, they will reflect, as appropriate, updated information on the CFDI, the status of relevant international agreements, and other international CIKR protection efforts.

Appendix 2: 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 CIKR protection. This list is not inclusive of all authorities related to CIKR protection; rather, it includes the authorities most relevant to national-level, cross-sector CIKR protection. Please note that there are many other authorities that are related to specific sectors that are not discussed in this appendix; these are left for further elaboration in the SSPs.

2.1 Statutes

Homeland Security Act of 2002[9]

This act establishes 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 assigns 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
- Ensure that the overall economic security of the United States is not diminished by efforts, activities, and programs aimed at securing the homeland.

This statutory authority defines the protection of CIKR as one of the primary missions of the department. Among other actions, the act specifically requires DHS:

- To carry out comprehensive assessments of the vulnerabilities of U.S. CIKR, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks;
- To develop a comprehensive national plan for securing the CIKR of the United States, including power production, generation, and distribution systems; IT and telecommunications systems (including satellites); electronic financial and property record storage and transmission systems; emergency preparedness communications systems; and the physical and technological assets that support such systems; and

[9] Public Law 107-296, November 25, 2002, 116 Stat. 2135. It is coded at 6 U.S.C.

- To recommend measures necessary to protect U.S. CIKR 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.

Those requirements, combined with the President's direction in HSPD-7, mandate the unified approach to CIKR protection taken in the NIPP.

Critical Infrastructure Information Act of 2002[10]

Enacted as part of the Homeland Security Act, this act creates a framework that enables members of the private sector and others to voluntarily submit sensitive information regarding the Nation's CIKR to DHS with the assurance that the information, if it satisfies certain requirements, will be protected from public disclosure.

The PCII Program, created under the authority of 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 CIKR protection efforts.[11]

Implementing Recommendations of the 9/11 Commission Act of 2007

This act requires the implementation of some of the recommendations made by the 9/11 Commission, to include requiring the Secretary of Homeland Security to: (1) establish department-wide procedures to receive and analyze intelligence from State, local, and tribal governments and the private sector; and (2) establish a system that screens 100 percent of maritime and passenger cargo.

Section 1002 of the act includes a requirement for DHS to report annually to Congress on the comprehensive risk assessments carried out for each CIKR sector, to include an evaluation of threats, vulnerabilities, and consequences. These reports should describe any actions or countermeasures recommended or taken by DHS or another SSA to address the issues identified in the assessments. This reporting requirement is covered by the National CIKR Protection Annual Report submitted to Congress in November of each year, as well as the Congressional Mid-Year Brief delivered to Congress each Spring.

This act establishes the International Border Community Interoperable Communications Demonstration Project, which helps identify and implement solutions to cross-border communications and cooperation, and the Interagency Threat Assessment and Coordination Group (ITACG), which improves interagency communications. The establishment of ITACG Advisory Councils allows Federal agencies to set policies to improve communication within the information-sharing environment and supports establishment of an ITACG Detail that gives State, local, and tribal homeland security officials, law enforcement officers, and intelligence analysts the opportunity to work in the National Counterterrorism Center.

The act also established grants to support high-risk urban areas and State, local, and tribal governments in preventing, preparing for, protecting against, and responding to acts of terrorism, and to assist States in carrying out initiatives to improve international emergency communications.

Title IX of the act requires DHS to establish a common set of criteria for private sector preparedness in disaster management, emergency management, and business continuity. These Voluntary Private Sector Preparedness Standards will be accredited and certified by ANSI and the ASQ ANAB. An internal DHS Private Sector Preparedness Council will be responsible for: selecting program standards; defining and promoting the business case for private sector entities to work toward voluntary certification; overseeing the program's progress; and providing regular updates to Congress.

Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act)[12]

The Stafford Act provides comprehensive authority for response to emergencies and major disasters—natural disasters, accidents, and intentionally perpetrated events. It provides specific authority for the Federal Government to provide assistance to State and local entities for disaster preparedness and mitigation, and major disaster and emergency assistance. Major disaster and emergency assistance includes such resources and services as:

[10] The CII Act is presented as subtitle B of title II of the Homeland Security Act (sections 211-215) and is codified at 6 U.S.C. 131 et seq.
[11] Procedures for Handling Critical Infrastructure Information, 68 Fed. Reg. 8079 (Feb. 20, 2004), are codified at 6 CFR Part 29.
[12] Public Law 93-288, as amended, codified at 42 U.S.C. 68.

- The provision of Federal resources, in general;
- Medicine, food, and other consumables;
- Work and services to save lives and restore property, including:
  - Debris removal;
  - Search and rescue; emergency medical care; emergency mass care; emergency shelter; and provision of food, water, medicine, and other essential needs, including movement of supplies or persons;
  - Clearance of roads and construction of temporary bridges;
  - Provision of temporary facilities for schools and other essential community services;
  - Demolition of unsafe structures that endanger the public;
  - Warning of further risks and hazards;
  - Dissemination of public information and assistance regarding health and safety measures;
  - Provision of technical advice to State and local governments on disaster management and control; and
  - Reduction of immediate threats to life, property, and public health and safety;
- Hazard mitigation;
- Repair, replacement, and restoration of certain damaged facilities; and
- Emergency communications, emergency transportation, and fire management assistance.

Disaster Mitigation Act of 2000

This act amends the Stafford Act by repealing the previous mitigation planning provisions (section 409) and replacing them with a new set of requirements (section 322). This new section emphasizes the need for State, local, and tribal entities to closely coordinate mitigation planning and implementation efforts.

Section 322 continues the requirement for a State mitigation plan as a condition of disaster assistance, adding incentives for increased coordination and integration of mitigation activities at the State level through the establishment of requirements for two different levels of State plans—standard and enhanced. States that demonstrate an increased commitment to comprehensive mitigation planning and implementation through the development of an approved Enhanced State Plan can increase the amount of funding available through the Hazard Mitigation Grant Program (HMGP). Section 322 also establishes a new requirement for local mitigation plans and authorizes up to 7 percent of HMGP funds available to a State to be used for development of State, local, and tribal mitigation plans.

Corporate and Criminal Fraud Accountability Act of 2002 (also known as the Sarbanes-Oxley Act)[13]

The act applies to entities required to file periodic reports with the Securities and Exchange Commission under the provisions of the Securities and Exchange Act of 1934, as amended. It contains significant changes to the responsibilities of directors and officers, as well as the reporting and corporate governance obligations of affected companies. Among other items, the act requires certification by the company's chief executive officer (CEO) and chief financial officer that accompanies each periodic report filed that the report fully complies with the requirements of the securities laws and that the information in the report fairly presents, in all material respects, the financial condition and results of the operations of the company. It also requires certifications regarding internal controls and material misstatements or omissions, and the disclosure on a "rapid and current basis" of information regarding material changes in the financial condition or operations of a public company. The act contains a number of additional provisions dealing with insider accountability and disclosure obligations, and auditor independence. It also provides severe criminal and civil penalties for violations of the act's provisions.

[13] Public Law 107-204, July 30, 2002.

The Defense Production Act of 1950 and the Defense Production Reauthorization Act of 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 require that companies accept and give priority to 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. This act also authorizes loan guarantees, direct loans, direct purchases, and purchase guarantees for those goods necessary for national defense. It also provides for the review of foreign acquisitions of U.S. businesses in order to identify and resolve any national security risks. This act defines "national defense" to include critical infrastructure protection and restoration, as well as activities authorized by the emergency preparedness sections of the Stafford Act. Consequently, the authority stemming from the Defense Production Act is available for activities and measures undertaken in preparation for, during, or following a natural disaster or accidental or malicious event. Under the act and related Presidential orders, the Secretary of Homeland Security has the authority to place and, upon application, authorize State and local governments to place priority-rated contracts for industrial resources in support of Federal, State, and local emergency preparedness activities. The Defense Production Act has a national security nexus with the NIPP.

The Freedom of Information Act[14]

This act generally provides that any person has a right, enforceable in court, to obtain access to Federal agency records, except to the extent that such records are protected from public disclosure by the nine listed exemptions or the three law enforcement exclusions. Persons who make requests are not required to identify themselves or explain the purpose of the request. The underlying principle of FOIA is that the workings of government are for and by the people and that the benefits of government information should be made broadly available. All Federal Government agencies must adhere to the provisions of FOIA with certain exceptions for work in progress, enforcement confidential information, classified documents, and national security information. FOIA was amended by the Electronic Freedom of Information Act Amendment of 1996 and the OPEN Government Act of 2007.

Information Technology Management Reform Act of 1996[15]

Under section 5131 of the Information Technology Management Reform Act of 1996, NIST develops standards, guidelines, and associated methods and techniques for Federal computer systems. Federal Information Processing Standards are developed by NIST 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 of 1999[16]

Among other items, this act (title V) provides limited privacy protections on the disclosure by a financial institution of nonpublic personal information. The act also codifies protections against the practice of obtaining personal information through false pretenses.

Public Health Security and Bioterrorism Preparedness and Response Act of 2002[17]

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 HHS 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.

[14] Codified as 5 U.S.C. 552.
[15] Public Law 104-106.
[16] Public Law 106-102 (1999), codified at 15 U.S.C. 94.
[17] Public Law 107-188.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)[18]

This act outlines the domestic policy related to deterring and punishing terrorists, and the U.S. policy for CIKR protection. It also provides for the establishment of a national competence for CIKR protection. The act establishes the NISAC and outlines the Federal Government's commitment to understanding and protecting the interdependencies among critical infrastructure.

The Privacy Act of 1974[19]

This act provides strict limits on the maintenance and disclosure by any Federal agency of information on individuals that is maintained, including "education, financial transactions, medical history, and criminal or employment history and that contains [the] name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." Although there are specific categories for permissible maintenance of records and limited exceptions to the prohibition on disclosure for legitimate law enforcement and other specified purposes, the act requires strict recordkeeping on any disclosure. The act also specifically provides for access by individuals to their own records and for requesting corrections thereto.

Federal Information Security Management Act of 2002[20]

This act requires 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.

Cyber Security Research and Development Act of 2002[21]

This act allocates funding to NIST and the National Science Foundation for the purpose 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 CIKR.

Maritime Transportation Security Act of 2002[22]

This act directs initial and continuing assessments of maritime facilities and vessels that may be involved in a transportation security incident. It requires DHS to prepare a National Maritime Transportation Security Plan for deterring and responding to a transportation security incident and to prepare incident response plans for facilities and vessels that will ensure effective coordination with Federal, State, and local authorities. It also requires, among other actions, the establishment of: transportation security and crewmember identification cards and processes; maritime safety and security teams; port security grants; and enhancements to maritime intelligence and matters dealing with foreign ports and international cooperation.

Atomic Energy Act of 1954

The Atomic Energy Act of 1954, as amended in NUREG-0980, provides for both the development and regulation of civilian uses of nuclear materials and facilities in the United States. The act requires that civilian uses of nuclear materials and facilities be licensed and it empowers the NRC to establish, by rule or order, standards to govern these uses.

Intelligence Reform and Terrorism Prevention Act of 2004[23]

This act provides sweeping changes to the U.S. Intelligence Community structure and processes, and creates new systems that are specially designed to combat terrorism. Among other actions, the act:

[18] Public Law 107-56, October 26, 2001.
[19] Codified at 5 U.S.C. 552a.
[20] Public Law 107-347, December 17, 2002.
[21] Public Law 107-305, November 27, 2002.
[22] Public Law 107-295, codified at 46 U.S.C. 701.
[23] Public Law 108-458.

- Establishes a Director of National Intelligence with specific budget, oversight, and programmatic authority over the Intelligence Community;
- Establishes the National Intelligence Council and redefines "national intelligence";
- Requires the establishment of a secure ISE and an information-sharing council;
- Establishes a National Counterterrorism Center, a National Counterproliferation Center, National Intelligence Centers, and a Joint Intelligence Community Council;
- Establishes, within the EOP, a Privacy and Civil Liberties Oversight Board;
- Requires the Director of the FBI to continue efforts to improve the intelligence capabilities of the FBI and to develop and maintain, within the FBI, a national intelligence workforce;
- Directs improvements in security clearances and clearance processes;
- Requires DHS to: develop and implement a National Strategy for Transportation Security and transportation modal security plans; enhance identification and credentialing of transportation workers and law enforcement officers; conduct R&D into mass identification technology, including biometrics; enhance passenger screening and terrorist watch lists; improve measures for detecting weapons and explosives; improve security related to the air transportation of cargo; and implement other aviation security measures;
- Directs enhancements to maritime security;
- Directs enhancements in border security and immigration matters;
- Enhances law enforcement authority and capabilities, and expands certain diplomatic, foreign aid, and military authority and capabilities for combating terrorism;
- Requires expanded machine-readable visas with biometric data; implementation of a biometric entry and exit system, and a registered traveler program; and implementation of biometric or other secure passports;
- Requires standards for birth certificates and driver's licenses or personal identification cards issued by States for use by Federal agencies for identification purposes and enhanced regulations for social security cards;
- Requires DHS to improve preparedness nationally, especially measures to enhance interoperable communications and to report on vulnerability and risk assessments of the Nation's CIKR; and
- Directs measures to improve assistance to and coordination with State, local, and private sector entities.

2.2 National Strategies and Implementation Plans

The National Strategy for Homeland Security (July 2002)

This strategy establishes the Nation's strategic homeland security objectives and outlines the six critical mission areas necessary to achieve those objectives. The strategy also provides a framework to align the resources of the Federal budget directly to the task of securing the homeland. The strategy specifies eight major initiatives to protect the Nation's CIKR, one of which specifically calls for the development of the NIPP.

National Strategy for Homeland Security (October 2007)

The updated strategy serves to guide, organize, and unify our Nation's homeland security efforts. It is a national strategy (not a Federal strategy) that articulates the approach to secure the homeland over the next several years. It builds on the first National Strategy for Homeland Security, issued in July 2002, and complements both the National Security Strategy issued in March 2006 and the National Strategy for Combating Terrorism, issued in September 2006. It reflects the increased understanding of threats confronting the United States, incorporates lessons learned from exercises and real-world catastrophes, and addresses ways to ensure long-term success by strengthening the homeland security foundation that has been built.

National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (February 2003)

This strategy identifies 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 provides a unifying organizational structure for CIKR protection and identifies specific initiatives related to the NIPP to drive near-term national protection priorities and inform the resource allocation process.

National Strategy to Secure Cyberspace (February 2003)

This strategy sets forth objectives and specific actions to prevent cyber attacks against America's CIKR, reduce nationally identified vulnerabilities to cyber attacks, and minimize damage and recovery time from cyber attacks. The strategy provides the vision for cybersecurity and serves as the foundation for the cybersecurity component of CIKR.

The National Strategy for Maritime Security (September 2005)

This strategy provides the framework to integrate and synchronize the existing department-level strategies and ensure their effective and efficient implementation, and integrates all Federal Government maritime security programs and initiatives into a comprehensive and cohesive national effort involving appropriate Federal, State, local, and private sector entities.

The National Strategy to Combat Weapons of Mass Destruction (December 2002)

This strategy provides policy guidance on combating WMD through three pillars:

- Counterproliferation to combat WMD use;
- Strengthened nonproliferation to combat WMD proliferation; and
- Consequence management to respond to WMD use.

The National Strategy for Combating Terrorism (September 2006)

This strategy provides a comprehensive overview of the terrorist threat and sets specific goals and objectives to combat this threat, including measures to:

- Defeat terrorists and their organizations;
- Deny sponsorship, support, and sanctuary to terrorists;
- Diminish the underlying conditions that terrorists seek to exploit; and
- Defend U.S. citizens and interests at home and abroad.

The National Intelligence Strategy of the United States of America (October 2005)

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 that 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.

The National Continuity Policy Implementation Plan (August 2007)

The National Continuity Policy Implementation Plan (NCPIP) identifies how the National Continuity Policy described in NSPD-51/HSPD-20 will be translated into action. The NCPIP is a comprehensive and integrated list of directives for the Federal Executive Branch to ensure the effectiveness and survivability of our national continuity capability. It is also an educational primer for State, local, tribal, and territorial governments and private sector partners that support the Nation's continuity capability.

2.3 Homeland Security Presidential Directives

HSPD-1: Organization and Operation of the Homeland Security Council (October 2001)

HSPD-1 establishes the Homeland Security Council and a committee structure for developing, coordinating, and vetting homeland security policy among executive departments and agencies. The directive provides a mandate for the Homeland Security Council to ensure the coordination of all homeland security-related activities among executive departments and agencies, and promotes the effective development and implementation of all homeland security policies. The Homeland Security Council is responsible for arbitrating and coordinating any policy issues that may arise among the different departments and agencies covered by the NIPP.

HSPD-2: Combating Terrorism Through Immigration Policies (October 2001)

HSPD-2 establishes 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 directs the Attorney General to create the Foreign Terrorist Tracking Task Force to ensure that, to the maximum extent permitted by law, Federal agencies 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 (March 2002)

HSPD-3 mandates 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 includes the requirement for a corresponding set of protective measures for Federal, State, and local governments to be implemented, depending on the threat condition. 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. For each threat condition, Federal departments and agencies are required to implement a corresponding set of protective measures.

HSPD-4: National Strategy to Combat Weapons of Mass Destruction (December 2002)

This directive outlines a strategy that includes three principal pillars: (1) Counterproliferation to Combat WMD Use, (2) Strengthened Nonproliferation to Combat WMD Proliferation, and (3) Consequence Management to Respond to WMD Use. It also outlines four cross-cutting functions 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 establishes 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 is the NIMS, an organizational framework for all levels of government, and the NRF, an operational framework for national incident response.

In this directive, the President designates the Secretary of Homeland Security as the principal Federal official for domestic incident management and empowers the Secretary to coordinate Federal resources used for prevention, preparedness, response, and recovery related to terrorist attacks, major disasters, or other emergencies. The directive assigns 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 directs 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.

HSPD-6: Integration and Use of Screening Information (September 2003)

HSPD-6 consolidates the Federal Government's approach to terrorist screening by establishing a Terrorist Screening Center. Federal departments and agencies are directed to provide terrorist information to the Terrorist Threat Integration Center, which

is then required to provide all relevant information and intelligence to the Terrorist Screening Center. 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, local, tribal, territorial, 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 establishes a framework for Federal departments and agencies to identify, prioritize, and protect CIKR from terrorist attacks, with an emphasis on protecting against catastrophic health effects and mass casualties. HSPD-7 mandates the creation and implementation of the NIPP and sets forth the roles and responsibilities for: DHS; SSAs; other Federal departments and agencies; and State, local, tribal, territorial, private sector, and other CIKR partners.

HSPD-8: National Preparedness (December 2003)

HSPD-8 establishes 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 mandates the development of the goal to guide emergency preparedness training, planning, equipment, and exercises, and to ensure that all entities involved adhere to the same standards. The directive calls for an inventory of Federal response capabilities and refines the process by which preparedness grants are administered, disbursed, and utilized at the State and local levels.

HSPD-9: Defense of U.S. Agriculture and Food (January 2004)

HSPD-9 establishes 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 outlines the essential pillars of our national biodefense program as: (1) threat awareness; (2) prevention and protection; (3) surveillance and detection; and (4) response and recovery. This directive describes these various disciplines in detail and sets forth objectives for further progress under the national biodefense program, highlighting key roles for Federal departments and agencies. The Secretary of Homeland Security is responsible for coordinating domestic Federal operations to prepare for, respond to, and recover from biological weapons attacks.

HSPD-11: Comprehensive Terrorist-Related Screening Procedures (August 2004)

HSPD-11 requires the creation of a strategy and implementation plan for a coordinated and comprehensive approach to terrorist screening 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 Standard for Federal Employees and Contractors (August 2004)

HSPD-12 establishes a mandatory, government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors to enhance security, increase governmental efficiency, reduce identity fraud, and protect personal privacy. The resulting mandatory standard was issued by NIST as the Federal Information Processing Standard Publication.

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 establishes a Maritime Security Policy Coordinating Committee to coordinate interagency maritime security policy efforts.

HSPD-14: Domestic Nuclear Detection (April 2005)

HSPD-14 establishes 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.

HSPD-15: War on Terror (March 2006)

HSPD-15 is classified. The objective of the directive is to improve government coordination in the global war on terror.

HSPD-16: Aviation Security Policy (June 2006)

HSPD-16 details a strategic vision for aviation security while recognizing ongoing efforts, and directs the production of a National Strategy for Aviation Security and supporting plans. The supporting plans address the following areas: aviation transportation system security; aviation operational threat response; aviation transportation system recovery; air domain surveillance and intelligence integration; domestic outreach; and international outreach. The strategy: sets forth U.S. Government agency roles and responsibilities; establishes planning and operations coordination requirements; and builds on current strategies, tools, and resources.

HSPD-17: Nuclear Materials Information Program (August 2006)

HSPD-17 is classified. The directive addresses an interagency effort managed by the Department of Energy to consolidate information from all sources pertaining to worldwide nuclear materials holdings and their security status into an integrated and continuously updated information management system.

HSPD-18: Medical Countermeasures Against Weapons of Mass Destruction (January 2007)

HSPD-18 builds on the vision and objectives articulated in the National Strategy to Combat Weapons of Mass Destruction and Biodefense for the 21st Century to ensure that the Nation's medical countermeasures research, development, and acquisitions efforts: target threats that pose the potential for a catastrophic impact on public health; yield a rapidly deployable and flexible capability to address existing and evolving threats; are part of an integrated WMD consequence management approach; and include the development of effective, feasible, and pragmatic concepts of operation for responding to and recovering from an attack. The directive designates the Secretary of Homeland Security to develop a strategic, integrated chemical, biological, radiological, and nuclear risk assessment that integrates the findings of the intelligence and law enforcement communities with input from the scientific, medical, and public health communities.

HSPD-19: Combating Terrorist Use of Explosives in the United States (February 2007)

HSPD-19 establishes a national policy and calls for the development of a national strategy and implementation plan on the prevention and detection of, protection against, and response to terrorist use of explosives in the United States. This directive mandates that the Secretary of Homeland Security coordinate with other Federal agencies to maintain secure information-sharing systems available to law enforcement agencies and other first-responders, to include best practices to enhance preparedness across governmental entities. The Secretary of Homeland Security is also responsible, in coordination with other Federal agencies, for Federal Government research, development, testing, and evaluation activities related to explosives attacks and the development of explosive render-safe tools and technologies.

HSPD-20: National Continuity Policy (May 2007)

HSPD-20 (also NSPD-51) establishes a comprehensive national policy on the continuity of Federal Government structures and operations, and designates a single National Continuity Coordinator who is responsible for leading the development and implementation of Federal continuity policies. This policy: establishes National Essential Functions; prescribes continuity requirements for all executive departments and agencies; and provides guidance for State, local, tribal, and territorial governments, and private sector organizations. This directive aims to ensure a comprehensive and integrated national continuity program that

will enhance the credibility of our national security posture and enable a more rapid and effective response to and recovery from a national emergency.

HSPD-21: Public Health and Medical Preparedness (October 2007)

HSPD-21 establishes a National Strategy for Public Health and Medical Preparedness. The Strategy draws key principles from the National Strategy for Homeland Security (October 2007), the National Strategy to Combat Weapons of Mass Destruction (December 2002), and Biodefense for the 21st Century (April 2004) that can be generally applied to public health and medical preparedness. Implementation of this strategy will transform our national approach to protecting the health of the American people against all disasters.

HSPD-22: Domestic Chemical Defense

HSPD-22 is classified. HSPD-22 establishes a national policy and directs actions to strengthen the ability of the United States to prevent, protect, respond to, and recover from terrorist attacks employing toxic chemicals and other chemical incidents.

HSPD-23: Cyber Security and Monitoring (January 2008)

HSPD-23 (also National Security Presidential Directive 54) formalizes the "Comprehensive National Cybersecurity Initiative" and a series of continuous efforts designed to establish a frontline defense (reducing current vulnerabilities and preventing intrusions), defend against the full spectrum of threats by using intelligence and strengthening supply chain security, and shape the future environment by enhancing our research, development, and education, as well as investing in leap-ahead technologies. The contents of HSPD-23 are classified.

HSPD-24: Biometrics for Identification and Screening to Enhance National Security (June 2008)

HSPD-24 establishes a framework to ensure that Federal executive departments and agencies use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information on individuals in a lawful and appropriate manner, while respecting their information privacy and other legal rights under U.S. law.

2.4 Other Authorities

Executive Order 13231, Critical Infrastructure Protection in the Information Age (October 2001) (amended by E.O. 13286, February 28, 2003)

Executive Order 13231 provides specific policy direction to ensure the protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems. It recognizes the important role that networked information systems (critical information infrastructure) play in supporting all aspects of our civil society and economy, and the increasing degree to which other critical infrastructure sectors have become dependent on such systems. It formally establishes as U.S. policy the need to protect against disruption of the operation of these systems and to ensure that any disruptions that do occur are infrequent, of minimal duration, manageable, and cause the least damage possible. This Executive Order specifically calls for the implementation of the policy to include "a voluntary public-private partnership, involving corporate and nongovernmental organizations." This Executive Order also reaffirms existing authorities and responsibilities assigned to various executive branch agencies and interagency committees to ensure the security and integrity of Federal information systems generally and of national security information systems in particular.

National Infrastructure Advisory Council

In addition to the foregoing, Executive Order 13231 (as amended by E.O. 13286 of February 28, 2003, and E.O. 13385 of September 29, 2005) also established the NIAC as the President's principal advisory panel on CIKR protection issues spanning all sectors. The NIAC is composed of not more than 30 members, appointed by the President, who are selected from the private sector, academia, and State and local governments, representing senior executive leadership expertise from the CIKR areas as delineated in HSPD-7.

The NIAC provides the President, through the Secretary of Homeland Security, with advice on the security of CIKR, both physical and cyber, that supports important sectors of the economy. It also has the authority to provide advice directly to the heads of other departments who have shared responsibility for CIKR protection, including HHS, DOT, and DOE. The NIAC is charged to improve the cooperation and partnership between the public and private sectors in securing critical infrastructure and advises on policies and strategies that range from risk assessment and management, to information sharing, to protective strategies and clarification of the roles and responsibilities between public and private sectors.

Executive Order 12382, President's National Security Telecommunications Advisory Committee (amended by E.O. 13286, February 28, 2003)

Executive Order 12382 creates the NSTAC, which provides to the President, through the Secretary of Homeland Security, information and advice from the perspective of the telecommunications industry with respect to the implementation of the National Security Telecommunications Policy.

Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions (amended by E.O. 13286, February 28, 2003)

Executive Order 12472 assigns NS/EP telecommunications functions, including wartime and non-wartime emergency functions, to the National Security Council, OSTP, Homeland Security Council, OMB, and other Federal agencies. This Executive Order seeks to ensure that the Federal Government has telecommunications services that will function under all conditions, including emergency situations. This Executive Order directs the NCS to assist the President, the National Security Council, the Homeland Security Council, the Director of OSTP, and the Director of the OMB in: (1) exercising the telecommunications functions and responsibilities set forth in the Executive Order; and (2) coordinating the planning for and provision of NS/EP communications for the Federal Government under all circumstances, including a crisis or emergency, an attack, recovery, and reconstitution.

Executive Order 12977, Interagency Security Committee (amended by E.O. 13286, February 28, 2003)

Executive Order 12977 directs the Interagency Security Committee to develop standards, policies, and best practices for enhancing the quality and effectiveness of physical security and the protection of nonmilitary Federal facilities in the United States. The Interagency Security Committee provides a permanent body to address continuing government-wide security for Federal facilities.

Appendix 3: The Protection Program

Appendix 3A: NIPP Core Criteria for Risk Assessments

The NIPP core criteria for risk assessments identify the characteristics and information needed to produce results that can contribute to cross-sector risk comparisons. This appendix provides information for developing new and modifying existing methodologies so they can be used to support national-level comparative risk assessment, incident response planning, resource prioritization, and protective measures development and implementation. This appendix summarizes the information provided in section 3.3, which can be referenced for additional details on these topics.

Many stakeholders conduct risk assessments to meet their own decisionmaking needs, using a broad range of methodologies. Whenever possible, DHS seeks to use information from stakeholders' assessments to contribute to an understanding of risks across sectors and regions throughout the Nation. To do this consistently, the challenge of minimizing the disparity in the approaches must be addressed through the core criteria identified below. These criteria include both the analytic principles that are broadly applicable to all parts of a risk methodology and specific guidance regarding the information needed to understand and address each of the three components of the risk equation: consequence, vulnerability, and threat.

The basic analytic principles ensure that risk assessments are:

- **Documented**: The methodology and the assessment must clearly document which information is used and how it is synthesized to generate a risk estimate. Any assumptions, weighting factors, and subjective judgments need to be transparent to the user of the methodology, its audience, and others who are expected to use the results. The types of decisions that the risk assessment is designed to support and the timeframe of the assessment (e.g., current conditions versus future operations) should be given.
- **Reproducible**: The methodology must produce comparable, repeatable results, even though assessments of different CIKR will be performed by different analysts or teams of analysts. It must minimize the number and impact of subjective judgments, leaving policy and value judgments to be applied by decisionmakers.
- **Defensible**: The risk methodology must be technically sound, making appropriate use of the professional disciplines relevant to the analysis, as well as be free from significant errors or omissions. The uncertainty associated with consequence estimates and confidence in the vulnerability and threat estimates must be communicated.

- **Complete**: The methodology must assess consequence, vulnerability, and threat for every defined risk scenario and follow the more specific guidance for each of these as given below.

Core Criteria Guidance for Consequence Assessments

- Document the scenarios assessed, tools used, and any key assumptions made.
- Estimate the number of fatalities, injuries, and illnesses, where applicable and feasible, keeping each separate estimate visible to the user.
- Estimate the economic loss in dollars, stating which costs are included (e.g., property damage losses, lost revenue, loss to the economy) and what duration was considered.
- If monetizing the human health consequences, document the value(s) used and the assumptions made.
- Consider and document any protective or consequence mitigation measures that have their effect after the incident has occurred, such as the rerouting of systems or HAZMAT or fire and rescue response.
- Describe the psychological impacts and mission disruption, where feasible.[24]

Core Criteria Guidance for Vulnerability Assessments

- Identify the vulnerabilities associated with: physical, cyber, or human factors (openness to both insider and outsider threats); critical dependencies; and physical proximity to hazards.
- Describe all protective measures in place and how they reduce the vulnerability for each scenario.
- In evaluating security vulnerabilities, develop estimates of the likelihood of an adversary's success for each attack scenario.
- For natural hazards, estimate the likelihood that an incident would cause harm to the asset, system, or network, given that the natural hazard event occurs at the location of interest for the risk scenario.

Core Criteria Guidance for Threat Assessments

- For adversary-specific threat assessments:[25]
  - Account for the adversary's ability to recognize the target and the deterrence value of existing security measures.
  - Identify attack methods that may be employed.
  - Consider the level of capability that an adversary demonstrates with regard to a particular attack method.
  - Consider the degree of the adversary's intent to attack the target.
  - Estimate threat as the likelihood that the adversary would attempt a given attack method against the target.
  - If threat likelihoods cannot be estimated, use conditional risk values (consequence times vulnerability) and conduct sensitivity analyses to determine how likely the scenario would have to be to support the decision.
- For natural disasters and accidental hazards:
  - Use best-available analytic tools and historical data to estimate the likelihood that these events would affect CIKR.

In addition to the guidance available in the NIPP, and as resources allow, DHS provides direct assistance to partners who are developing and modifying risk methodologies. To discuss the possibility of such assistance, contact DHS at NIPP@dhs.gov.

[24] The assessment of the psychological impacts and mission disruption are currently maturing capabilities. Mission disruption is an area of strong NIPP partner interest for collaborative development of the appropriate metrics to help quantify and compare different types of losses. While development is ongoing, qualitative descriptions of the consequences are a sufficient goal.

[25] Threat information can be received through HSIN.

Appendix 3B: Existing CIKR Protection Programs and Initiatives

This appendix provides examples of the Federal programs that currently support NIPP implementation. The examples provided herein generally cut across sectors and have national significance. These Federal programs augment the extensive State, local, tribal, territorial, and private sector protection programs that constitute important efforts already being implemented in support of the NIPP. The SSPs address sector-specific programs that are conducted under the leadership of the SSAs, and include selected protection programs undertaken by other CIKR partners that are applicable across the sector.

3B.1 Programs and Initiatives

Site Assistance Visits (SAVs): SAVs are facility vulnerability assessments jointly conducted by DHS in coordination and collaboration with Federal, State, and local stakeholders, and CIKR owners and operators. The SAV uses a hybrid methodology of dynamic and static vulnerabilities, including elements of asset-based approaches (identifying and discussing critical site assets and current CIKR protection postures) and scenario-based approaches (assault planning and likely attack scenarios) to ensure that current threats are included. Through SAVs, DHS advises CIKR owners and operators about vulnerabilities, provides recommended protective measures that would increase the ability to deter or prevent terrorist attacks, and provides recommendations for reducing vulnerabilities or enhancing resiliency. An SAV can range from a "quick look" visit to a full security vulnerability assessment that takes 3 to 5 days to comprehensively review physical, cyber, and system interdependencies.

Buffer Zone Protection Program (BZPP): The BZPP is a DHS-administered grant program designed to increase security in the "buffer zone" (the area outside of a facility that can be leveraged by an adversary to conduct target surveillance or launch an attack). The BZP is a strategic document that is developed by the responsible local law enforcement jurisdictions that identifies significant aspects of the site that may be targeted by terrorists, identifies specific threats and vulnerabilities associated with the site, and develops an appropriate buffer zone extending outward from the facility in which protective measures can be employed to make it more difficult for terrorists to conduct site surveillance or launch attacks.

Comprehensive Reviews (CRs): The CR is a cooperative government-led assessment of CIKR facilities. The CR considers not only potential terrorist methods of attack, the consequences of such an attack, integrated preparedness and response capabilities of the owner/operator, LLE, and emergency response organizations, but also preparedness and response in the context of a natural disaster. The results are used to enhance the overall security and preparedness posture of the facilities, their surrounding communities, the geographic region, and ultimately the Nation. The CR provides a forum for candid and open dialogue among all levels of government and private sector. The CR incorporates a variety of assessment and exercise tools. Information obtained from the CR is used not only to enhance the capabilities of CIKR owner/operators and community first-responders, but also to provide risk data to inform Federal investment and R&D decisions.

Characteristics and Common Vulnerabilities, Potential Indicators of Terrorist Activity, and Protective Measures Reports: These reports identify common vulnerabilities by asset class within the sectors, as well as the types of terrorist activities that are likely to be successful in exploiting these vulnerabilities. They also identify security and preparedness best practices by asset class within the sectors. Integrated Infrastructure Papers integrate these reports and are currently available to more than 500 Federal, State, local, and private sector partners on a secure Web site.

Computer-Based Assessment Tool (CBAT): CBAT is an extension of the technical assistance provided for the DHS SAV Program and BZPP and is in support of designated special events. CBAT comprises technology and services that help DHS, owners and operators, local law enforcement, and emergency personnel prepare for, respond to, and manage special events. By integrating SAV and BZPP assessment data with geospherical video and geospatial and hypermedia data, CBAT provides planners with a computer-based, cross-platform tool that allows them to present data, make informed decisions quickly, and confidently respond to an incident. The "video walkthrough" of the facility or perimeter provided by CBAT also gives emergency response personnel a view of what they will encounter onsite. The system combines six individual, high-resolution cameras that provide a 360-degree spherical color video of the facilities, routes, and specific areas pertaining to a CBAT request.

Control Systems Security Initiative: DHS sponsors programs to increase the security of Internet-based control systems. A control system comprises components (designed to maintain the operation of a process or system) that are 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 CIKR and may be increasingly vulnerable to cyber threats that could have a devastating impact. The DHS Control Systems Security Initiative provides coordination 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 CIKR sectors.

Federal Cyber System Security Programs: DHS established the GFIRST to facilitate interagency information sharing and cooperation across the Federal agencies responsible for cyber system readiness and response. GFIRST members work together to understand and manage computer security incidents and encourage proactive and preventive security practices. Other examples of Federal agency cybersecurity access control, certification, and policy enforcement tools include:

- The General Services Administration (GSA) is responsible for developing and implementing an infrastructure for authentication services, as well as an automated risk assessment tool for government-wide use in certifying and accrediting its eAuthentication gateway. 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 (NOAA) has implemented enterprise-wide vulnerability assessments and virus-detection software, an intrusion-detection system, anti-virus scanning gateways, and a patch management policy.

Federal Hazard Mitigation Programs: FEMA administers three programs that provide funds for activities that reduce the losses from future disasters or help prevent the occurrence of catastrophes. These hazard mitigation programs include the Flood Mitigation Assistance Program, the Hazard Mitigation Grant Program, and the Pre-Disaster Mitigation Program. These programs enable grant recipients to undertake activities such as the elevation of structures in floodplains, the relocation of structures from floodplains, the construction of structural enhancements to facilities and buildings in earthquake-prone areas (also known as retrofitting), and modifications to land-use plans to ensure that future construction ameliorates hazardous conditions.

International Outreach Program: DHS works with DOS and other CIKR partners to conduct international outreach with foreign countries and international organizations to encourage the promotion and adoption of best practices, training, and other

programs, as needed, to improve the protection of overseas assets and to help ensure the reliability of the foreign infrastructure on which the United States depends.

National Cyber Exercises: DHS conducts exercises to identify, test, and improve coordination of the cyber incident response community, including Federal, State, local, tribal, territorial, and international governmental entities, as well as private sector corporations and coordinating councils.

National Cyber Response Coordination Group (NCRCG): This entity facilitates coordination of the Federal Government's efforts to prepare for, respond to, and recover from cyber incidents and physical attacks that have significant cyber consequences (collectively known as "cyber incidents"). The NCRCG serves as the Federal Government's principal interagency mechanism for operational information sharing and coordination of the Federal Government's response and recovery efforts during a cyber crisis. It uses established relationships with the private sector and State and local governments to help manage a cyber crisis, develop courses of action, and devise appropriate response and recovery strategies.

Protective Security Advisor (PSA) Program: DHS protection specialists are assigned as liaisons between DHS and the protective community at the State, local, and private sector levels in geographical areas representing major concentrations of CIKR across the United States. The PSAs are responsible for sharing risk information and providing technical assistance to local law enforcement and CIKR owners and operators of CIKR within those areas. They also serve an important role in facilitating the CIKR-related aspects of incident management operations under the NRF.

Software Assurance: DHS is developing best practices and new technologies to promote integrity, security, and reliability in software development. Focused on shifting away from the current security paradigm of patch management, DHS is leading the Software Assurance Program, a comprehensive strategy that addresses processes, technology, and acquisition throughout the software life cycle to result in secure and reliable software that supports critical mission requirements.

3B.2 Guidelines, Reports, and Planning

Cybersecurity Planning: DHS recognizes that each sector will have a unique reliance on cyber systems and will, therefore, assist SSAs in considering a range of effective and appropriate cyber protective measures. The sector-level approaches to cybersecurity will be documented in the respective SSPs.

Educational Reports: DHS provides several types of informational reports to support efforts to protect CIKR. They cover subjects such as CIKR common vulnerabilities, potential indicators of terrorist activity, and best practices for protective measures. As they are developed, these reports are distributed to all State and Territorial Homeland Security Offices with the guidance that they should be shared with CIKR owners and operators, the law enforcement community, and captains of the ports in their respective jurisdictions.

Risk Management Manuals: In response to the September 11, 2001 attacks, FEMA's role was expanded to include activities to reduce the vulnerability of buildings to terrorist attacks. In support of this mission, FEMA created the Risk Management Series, a collection of publications directed toward providing design guidance to mitigate the consequences of manmade disasters.

To date, the series includes the following manuals:

- FEMA 155, Building Design for Homeland Security
- FEMA 426, Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings
- FEMA 427, Primer for the Design of Commercial Buildings to Mitigate Terrorist Attacks
- FEMA 428, Primer to Design Safe School Projects in Case of Terrorist Attacks
- FEMA 429, Insurance, Finance, and Regulation Primer for Terrorism Risk Management in Buildings
- FEMA 430, Primer for Incorporating Building Security Components in Architectural Design
- FEMA 452, Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings
- FEMA 453, Multihazard Shelter (Safe Havens) Design

3B.3 Information-Sharing Programs That Support CIKR Protection

Federal agencies and the law enforcement community provide information-sharing services and programs that support CIKR protection information sharing. These include:

- **DHS Homeland Security Information Network (HSIN)**: HSIN is a national, Web-based communications platform that allows: DHS; SSAs; State, local, tribal, and territorial governmental entities; and other partners to obtain, analyze, and share information based on a common operating picture of strategic risk and the evolving incident landscape. The network is designed to provide a robust, dynamic information-sharing capability that supports both NIPP-related steady-state CIKR protection and NRF-related incident management activities, and to provide the information-sharing processes that form the bridge between these two homeland security missions. HSIN is one part of the ISE called for by the Intelligence Reform and Terrorism Prevention Act of 2004. As specified in the act, it will provide users with access to terrorism information that is matched to their roles, responsibilities, and missions in a timely and responsive manner. HSIN is discussed in detail in chapter 4. HSIN-Critical Sectors is an information-sharing portal designed to encourage communication and collaboration among all CIKR sectors and the Federal government. The content is tailored for each of the CIKR sectors.
- **FBI's InfraGard**: InfraGard is an information-sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the FBI and the private sector. InfraGard is an association of businesses, academic institutions, State and local law enforcement agencies, and other participants dedicated to sharing information and intelligence related to the protection of U.S. CIKR from both physical and cyber threats. InfraGard chapters are geographically linked with FBI Field Offices. Each InfraGard chapter has an FBI Special Agent Coordinator who works closely with Supervisory Special Agent Program Managers in the Cyber Division at FBI Headquarters.
- **Interagency Cybersecurity Efforts**: Interagency cooperation and information sharing are essential to improving national counterintelligence and law enforcement capabilities pertaining to cybersecurity. The intelligence and law enforcement communities have various official and unofficial information-sharing mechanisms in place. Examples include:
  - *U.S. Secret Service's Electronic Crimes Task Forces (ECTFs)*: These ECTFs provide interagency coordination on cyber-based attacks and intrusions. At present, 15 ECTFs are in operation, with an expansion planned.
  - *FBI's Inter-Agency Coordination Cell*: The Inter-Agency Coordination Cell is a multi-agency group focused on sharing law enforcement information on cyber-related investigations.
  - *Computer Crime and Intellectual Property Section*: The DOJ, Criminal Division, Computer Crime and Intellectual Property Section is responsible for prosecuting nationally significant cases of cyber crime and intellectual property crime. In addition to its direct litigation responsibilities, the division formulates and implements criminal enforcement policy and provides advice and assistance.
- **Law Enforcement Online (LEO)**: The FBI provides LEO as a national focal point for electronic communications, education, and information sharing for the law enforcement community. LEO, which can be accessed by any approved employee of a Federal, State, or local law enforcement agency, or approved member of an authorized law enforcement special interest group, is intended to provide a communications mechanism to link all levels of law enforcement throughout the United States.
- **Regional Information Sharing Systems (RISS)**: The RISS program is a federally funded program administered by the DOJ, Office of Justice Programs, Bureau of Justice Assistance. RISS serves more than 8,100 member law enforcement agencies in 50 States, the District of Columbia, Guam, Puerto Rico, the U.S. Virgin Islands, Australia, Canada, and the United Kingdom. The program comprises six regional centers that share intelligence and coordinate efforts against criminal networks that operate in many locations across jurisdictional lines. Typical targets of RISS activities are terrorism, drug trafficking, violent crime, cyber crime, gang activity, and organized criminal activities. The majority of the member agencies are at the municipal and county levels; however, more than 485 State agencies and more than 920 Federal agencies also participate. The Drug Enforcement Administration; FBI; U.S. Attorneys' Offices; Internal Revenue Service; Secret Service; U.S. Immigration and Customs Enforcement; and the Bureau of Alcohol, Tobacco, Firearms, and Explosives are among the Federal agencies participating in the RISS program.

- **Sharing National Security Information**: The ability to share relevant classified information poses a number of challenges, particularly when the majority of industry facilities are neither designed for nor accredited to receive, store, and dispose of these materials. Ultimately, HSIN may be used to more efficiently share appropriate classified national security information with cleared private sector owners and operators during incidents, times of heightened threat, or on an as-needed basis. While supporting technologies and policies are identified to satisfy this requirement, DHS will continue to expand its initiative to sponsor security clearances for designated private sector owners and operators, sharing classified information using currently available methods.
- **Web-Based Services for Citizens**: A variety of Web-based information services are available to enhance the general awareness and preparedness of American citizens. These include CitizenCorps.gov, FirstGov.gov, Ready.gov, and USAonwatch.org.

Appendix 3C: Infrastructure Data Warehouse

3C.1 Why Do We Need a National CIKR 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 CIKR 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. This inventory is also essential to help inform decisionmaking and specific response and recovery activities pertaining to natural disasters and other emergencies.

To fulfill this need, DHS has developed the federated IDW, a continually evolving and comprehensive catalog of the assets, systems, and networks that make up the Nation's CIKR. The IDW enables access to descriptive information regarding CIKR. Although the IDW is not a listing of prioritized assets, it has the capability to help inform risk-mitigation activities across the CIKR sectors and government jurisdictions.

3C.2 How Does the Inventory Support the NIPP?

The IDW provides a coordinated and consistent framework to access and display the CIKR data submitted by: Federal, State, and local agencies; the private sector; and integrated Federal or commercial databases. The federated framework and structure of the IDW have been constructed to readily integrate other CIKR data sources and provide the required data in a usable and effective manner. Two primary components of this framework are the Infrastructure Protection Taxonomy and infrastructure type data fields:

- The IP taxonomy groups CIKR by sector and identifies overlaps between and across sectors. It was developed by DHS in coordination with the SSAs to ensure that every CIKR 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 CIKR, making the IDW compliant with the National Information Exchange Model (NIEM). The information contained in these data fields feeds the strategic risk assessment process used to prioritize CIKR in the context of terrorist threats or incidents, natural disasters, or other emergencies.

The information accessed through the IDW supports the analysis to determine which assets, systems, and networks make up the Nation's CIKR and to inform security planning and preparedness, resource investments, and post-incident response and recovery activities within and across sectors and governmental jurisdictions.

3C.3 What Is the Current Content of the Inventory?

DHS gathers data related to the Nation's CIKR from a variety of sources. The inventory reflects a collection of information garnered from formal data calls, voluntary additions, and the leveraging of various Federal and commercial databases. Information accessed through the IDW has been received from Federal agencies, State and local submissions, voluntary private sector submissions, commercial demographics products, external data sources, and subject matter experts. The information is used to inform CIKR protection efforts, contingency planning, and planning for implementation of initiatives such as the BZPP, and to aid decisionmakers during response and recovery following terrorist attacks, natural disasters, or other emergencies.

3C.4 How Will the Current Inventory Remain Accurate?

DHS continues to seek input from multiple infrastructure sources, including existing databases managed by SSAs, commercial providers, State and local governments, and the private sector. Integrating existing databases using a federated framework will provide a dynamic common operating interface of infrastructure and vulnerability information through a cross-flow of data between separate databases or linked 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 Original Classification Authority (OCA) guidance and will be protected as required by OCA guidance and direction.

Table 3C-1: Database Integration

Database	Use
Integrated Common Analytical Viewer (iCAV)	DHS is leveraging existing geospatial capabilities and technology used by the National Geospatial-Intelligence Agency by implementing the iCAV as a DHS Geospatial Enterprise Solution for geospatial mapping, analysis, and sorting of the Nation's CIKR. The iCAV system will use the geospatial component to spatially display and map CIKR information.
National Threat Incident Database	This database provides a source of consolidated information concerning credible threats and incidents related to our Nation's CIKR.
DHS LENS Vulnerability Databases	These databases contain Characteristics and Common Vulnerabilities and Potential Indicators of Terrorist Activity Reports, and Site Assistance Visits and BZPP schedules. Site Assistance Visits and BZPP documents will be available through classified and unclassified secure portals as applicable.
Commercial/Sector-Specific Databases	Many existing Federal and commercial databases contain information sets pertinent to the CIKR mission. Commercial databases will be purchased based on available funding and priorities for information requirements.

3C.5 How Will the Infrastructure Data Warehouse Be Maintained?

The process of ensuring that the data collected is both current and accurate is continual. Data updates and currency are largely dependent on the sources of the data and the frequency of the updates that they provide.

Efficiency and reliability are maintained through the implementation of various data quality control techniques. Verification and validation efforts by contracted companies or Federal employees will play a key role in ensuring information currency.

3C.6 How Do CIKR Partners Contribute?

The CIKR information accessible through the IDW is highly dependent on the participation and support of the SSAs, the States, and private sector entities:

- SSAs have the primary responsibility for providing sector information to DHS for inclusion in the IDW.[26] The processes used for sector CIKR and database identification in coordination with partners should be described in the SSPs.
- Some State governments have either already developed infrastructure databases or have begun the process to identify and assess CIKR within their jurisdictions. State Homeland Security Advisors should work closely with DHS and the SSAs to ensure that data collection efforts are streamlined, coordinated, and reflect the most accurate data possible.
- The most current and accurate data are best known by CIKR owners and operators. Thus, as the owners and operators of the majority of the Nation's CIKR, private sector entities are encouraged to be actively involved in the development of CIKR information.

3C.7 What Are the Plans for IDW Expansion?

Planned advancements include integration with multiple commercial and Federal CIKR databases, vulnerability assessment tools and libraries, intelligence and threat reporting databases, and geospatial tools.

DHS is developing the IDW with a versatile platform to support integration of DHS and SSA applications and databases. The goal of this effort is to create a means for appropriate parties to access national CIKR information that more efficiently and effectively supports the implementation of NIPP risk management framework activities, including:

- Integration of vulnerability, consequence, and asset/system/network attribute data into a single portal interface as the foundation for the NIPP risk assessment process;
- Access to threat data to support the development of asset, system, and network risk scores;
- Assessment and, if appropriate, prioritization of assets, systems, and networks across sectors and jurisdictions based on risk to promote the more effective allocation and use of available resources and to inform planning, threat response, and post-incident restoration actions at all levels of government and the private sector;
- Sharing of consistent information so that all partners involved in CIKR protection operate from a common frame of reference;
- Acting as a primary information and integration hub for protective security needs throughout the country in support of DHS- and SSA-led activities;
- Supporting the efforts of law enforcement agencies during National Security Special Events and other high-priority security events; and
- Supporting the efforts of primary Federal agencies in responding to and recovering from major natural or manmade disasters.

[26] The IP Taxonomy is the foundation for multiple DHS programs that focus on CIKR, such as the IDW and the National Threat Incident Database, and should provide the foundation for the lexicon used in 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.

Appendix 4: Existing Coordination Mechanisms

The coordination mechanisms established under the NIPP serve as the primary means for coordinating CIKR protection activities nationally. However, many other avenues exist for CIKR partners to engage with each other and government at all levels to ensure that their efforts are fully coordinated in accordance with the principles outlined in the NIPP. The following table summarizes many of these available mechanisms.

Coordination	Mechanism	Description
Local to Local	Interlocal Agreements	Cities and towns exchange information and cooperate on any number of projects. Interlocal 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 can receive assistance at 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 coordinating the relevant terms and conditions in advance.
	County Commissioner Interaction	County commissioners provide leadership, services, and programs to meet the health, safety, and welfare needs of their citizens in an integrated, collaborative network.
Local to State	Committees, Commissions, and Boards	Local-to-State legislative- and regulatory-level interactions occur through State committees, commissions, and boards dealing with counterterrorism, environmental, transportation, community development, retirement, insurance, and many other issues. Interactions also include coordination among the Office of the Governor, the Homeland Security Advisor, the Emergency Management Agency, and the National Guard.
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 the 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 appropriately targeted 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, rural development, and various other needs.
	Interstate or Regional Compacts (including those with cross-border entities)	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 CIKR. Compacts are organized in a number of ways: • Sector-based compacts focus on specific CIKR 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 individual State and local governments. • Regional compacts provide a means for participating jurisdictions to coordinate activities within a specific geographical area that spans multiple States. These agreements, such as the Canadian River Compact, define the specific equities of each State within the particular region. For more information on interstate compacts, contact the National Center for Interstate Compacts through their Web site at www.csg.org/programs/ncic/default.aspx.

Coordination	Mechanism	Description
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 the States in the Federal policymaking process. State-level professional associations, such as the Association of State Drinking Water Administrators and the Association of State and Interstate Water Pollution Control Administrators, also provide sector-specific coordination mechanisms; there are similar associations for each of the sectors. Additionally, these groups support State leaders by keeping their members informed of key Federal decisions that affect State government.
	State Liaison Offices	Some States have formed specific liaison offices in Washington, DC, to maintain awareness of Federal developments and to ensure that their individual State's 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.
	State and Local Fusion Centers (SLFCs)	The DHS Office of Intelligence and Analysis (I&A) places intelligence analysts in SLFCs to provide a coherent point of information exchange and intelligence sharing among the Federal Government and State, local, and tribal governments. In addition, the PSA Program is deploying field-based Protective Security Advisor Analysts to select SLFCs throughout the country. Their focus will be to analyze risks to CIKR in the region relative to current intelligence and to aid State, local, and private sector representatives in prioritizing CIKR protection efforts.
Federal to Federal	Memoranda of Understanding or Agreement	Agreements among two or more Federal departments and agencies to cooperate on a specific topic or initiative.
	Interagency Security Committee	The ISC is a permanent body of senior representatives from all branches of the government that addresses continuing government-wide security for Federal facilities.
Private Sector to Government (all levels)	Public-Private Partnerships	A public-private partnership is a 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 providing a 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 CIKR 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 government 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 made up 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 learn about the concerns of specific groups of CIKR partners. In addition, many associations serve as standard-setting organizations for their sectors.

Appendix 5: Integrating CIKR Protection as Part of the Homeland Security Mission

Appendix 5A: State, Local, Tribal, and Territorial Government Considerations

State, local, tribal, and territorial efforts support the implementation of the NIPP and associated SSPs by providing a jurisdictional focus and enabling cross-sector coordination. The NIPP recognizes that there is not a one-size-fits-all approach to CIKR protection planning at the State and local levels. Creating and managing a CIKR 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 action within the jurisdiction to set goals and objectives; identify assets, systems, and networks; assess risks; prioritize CIKR across sectors; implement protective programs and resiliency strategies; and measure the effectiveness of risk-mitigation efforts. These elements form the basis of CIKR protection programs and guide the implementation of relevant CIKR protection-related goals and objectives outlined in State, local, tribal, and territorial homeland security strategies.

This appendix provides general guidance that can be tailored to: unique jurisdictional characteristics; organizational structures; and operating environments at the State, local, tribal, and territorial levels. Additional guidance is available in A Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal, and Territorial Levels (2008). This guide can be accessed at www.dhs.gov/nipp.

The NIPP is structured to avoid redundancy and to ensure coordination among Federal, State, and local CIKR protection efforts. States or localities are encouraged to focus their efforts in ways that leverage Federal resources and address the relevant CIKR sector's protection requirements in their particular areas or jurisdictions. This appendix outlines a basic framework to guide the development of CIKR protection strategies, plans, and programs in coordination with the NIPP.

To be in alignment with the NIPP, State and local CIKR protection plans and programs should explicitly address six broad categories:

- CIKR protection roles and responsibilities;
- Partnership building and information sharing;
- Implementation of the NIPP risk management framework;
- CIKR data use and protection;

- Leveraging of ongoing emergency preparedness activities for CIKR protection; and
- Integration of Federal CIKR protection and resiliency activities.

5A.1 CIKR Roles and Responsibilities

The NIPP outlines a set of broad roles and responsibilities for State, local, tribal, territorial, and regional entities (see chapter 2). State, local, tribal, territorial, and regional CIKR protection plans (or entities addressing CIKR in State or local homeland security plans or strategies) should describe how each jurisdiction intends to implement these roles and responsibilities. In particular, jurisdictions should consider and describe in their plans the following:

- Which offices or organizations in the jurisdiction perform the roles or responsibilities outlined in the NIPP or the supporting SSPs;
- Whether gaps exist between the jurisdiction's current approach and those roles and responsibilities outlined in the NIPP or in an SSP, and how the gaps will be addressed;
- Whether any roles and responsibilities should be revised, modified, or consolidated to accommodate the unique operating attributes of the jurisdiction;
- How the jurisdiction will maintain operational awareness of the performance of the CIKR protection roles assigned to different offices, agencies, or localities; and
- How the jurisdiction will coordinate its CIKR protection roles and responsibilities with other jurisdictions and the Federal Government.

5A.2 Partnership Building and Information Sharing

Effective CIKR protection requires the development of partnerships, collaboration, and information sharing between government and CIKR owners and operators. This includes maintaining awareness of CIKR owner and operator concerns, disseminating relevant information to owners and operators, and maintaining processes for rapid response and decisionmaking in the event of a threat or incident involving CIKR within the jurisdiction. To address partnership building, networking, and information sharing, State and local entities should determine whether the appropriate mechanisms for sharing information and networking with CIKR partners are in place. If mechanisms are not established at all of the relevant levels, State and local entities should identify the means for better coordinating and sharing information with CIKR partners. Options to be considered and described in State, local, tribal, territorial, and regional CIKR protection plans can include, but are not limited to:

- Ensuring collaboration with other governmental entities and the private sector using a process based on the partnership model outlined under the NIPP or an abbreviated form of the model that addresses only those sectors that are most relevant to the jurisdiction;
- Instituting specific information-sharing networks, such as an information-sharing portal, for the jurisdiction. These types of networks allow owners and operators, and governmental entities to share best practices, provide a better understanding of sector and cross-sector needs, and inform collective decisionmaking on how best to utilize resources;
- Utilizing SLFCs, where applicable. SLFCs coordinate the collection, analysis, and dissemination of law enforcement, homeland security, public safety, and terrorism information;
- Developing standing committees and work groups to discuss relevant CIKR protection issues;
- Developing a regular newsletter or similar communications tool for CIKR owners and operators on relevant CIKR protection issues and coordination within the jurisdiction; and
- Participating in existing sector-wide and national information-sharing networks, including those offered by trade associations, ISACs, SCCs, and threat warning and alert notification systems.

The information-sharing approach for a given jurisdiction will vary based on CIKR ownership, the number and type of CIKR 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 CIKR protection plan.

5A.3 Implementing the Risk Management Framework

The NIPP risk management framework described in chapter 3 provides a useful model for State, local, tribal, territorial, and regional jurisdictions to use in addressing CIKR protection within the given jurisdiction. The model provides a risk-informed approach to identify, prioritize, and protect CIKR assets and systems at the State and local level. This process also allows State and local jurisdictions to enhance coordination with DHS and the SSAs in developing and implementing CIKR protection programs. The following should be considered when developing CIKR protection programs:

- What are the jurisdiction's goals and objectives for CIKR protection? How do these goals relate to those of the NIPP and the SSPs that are relevant to the jurisdiction?
- What are the CIKR assets, systems, and networks within the jurisdiction or that affect the jurisdiction? Are there significant interstate or international dependencies or interdependencies? Are any of the assets, systems, or networks within the jurisdiction deemed to be nationally critical by DHS?
- Are risk assessments for CIKR within the State being conducted or planned by DHS, the 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 CIKR protection priorities within the jurisdiction? How do these priorities correlate with the national priorities established by the Federal Government? How do these priorities correlate with the ongoing CIKR protection priorities established for each sector at the national level?
- What actions or initiatives are being taken within the jurisdiction to address CIKR protection and resiliency? How do these relate to the national effort?
- What types of metrics will be used to measure the progress of CIKR protection efforts?

5A.4 CIKR Data Use and Protection

States and other jurisdictions may employ a variety of means to collect CIKR data or respond to CIKR data requests. State, local, tribal, territorial, and regional plans should outline how the jurisdiction has organized itself to address CIKR data use and protection. The following issues should be considered in developing the CIKR protection plan:

- Will the jurisdiction maintain a comprehensive database of CIKR in the State, region, or locality? How will the jurisdiction collect such information? What tools are available from DHS or in the commercial marketplace to support infrastructure information collection and management?
- How will sensitive data that may be in the possession of State, local, tribal, or territorial governments be legally and physically protected from public disclosure and what safeguards will be used to control and limit distribution to the appropriate individuals?
- Will data collection mechanisms be compatible and interoperable with the IDW framework to enable data sharing?
- How will the jurisdiction ensure that it is maintaining current information?
- Will data requests from the Federal Government for CIKR data be channeled to the owners and operators through the States?
- 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?

5A.5 Leveraging of Ongoing Emergency Preparedness Activities for CIKR Protection

The emergency management capabilities of each State and local jurisdiction are an important component of improving overall CIKR protection. States and localities should look to existing programs and leverage ways in which CIKR protection can be integrated into ongoing activities. Areas to be considered when drafting a CIKR protection plan include:

- Does the jurisdiction's exercise program account for CIKR protection? If not, how will the State or locality incorporate CIKR protection exercise scenarios to increase the level of preparedness?
- Does the State Preparedness Report account for CIKR protection?
- How do CIKR 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 CIKR protection initiatives?
- How will the jurisdiction share best practices, reports, or other output from emergency preparedness activities with CIKR owners and operators?
- Have CIKR owners and operators been invited to participate in exercise events and are CIKR owners and operators linked to existing warning or response systems?
- What existing educational and outreach programs can be leveraged to share information with partners regarding CIKR protection?
- Are there other outreach or emergency management programs that should include a CIKR component?

5A.6 Integrating Federal CIKR Protection Activities

State-, local-, tribal-, and territorial- level CIKR protection programs should complement and draw on Federal efforts to the maximum extent possible to utilize risk management methodologies and avoid the duplication of efforts.

State, local, tribal, and territorial efforts should consider the adequacy of DHS and SSA guidance and resources for their particular situation. For example:

- Are the existing criteria for risk analysis inclusive of levels of consequence 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?
- Are there additional best practices that should be shared among CIKR partners?
- Are there additional authorities that need to be documented?

Appendix 5B: 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 CIKR protection programs. The recommendations herein are based on best practices in use by various sectors and other groupings. The NIPP encourages private sector owners and operators to adopt and implement those practices that are appropriate and applicable at the enterprise and individual facility levels. These may include:

- Asset, System, and Network Identification:
  - Incorporate the NIPP framework for the assets, systems, and networks under their control; and
  - Voluntarily share CIKR-related information with the appropriate partners to facilitate CIKR protection program implementation with applicable information protections.
- Assessment, Monitoring, and Reduction of Risks/Vulnerabilities:
  - 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 corresponding to the physical, cyber, and human security elements of CIKR protection;
  - Maintain the tools, capabilities, and protocols necessary to provide an appropriate level of monitoring of networks, systems, or a facility and its immediate surroundings to detect possible insider and external threats;
  - Develop and implement personnel screening programs to the extent feasible for personnel working in sensitive positions; and
  - Manage the security of computer and information systems while maintaining awareness of vulnerabilities and consequences to ensure that systems are not used to enable attacks against CIKR.

- Information Sharing:
  - Connect with and participate in the appropriate national, State, regional, local, and sector information-sharing mechanisms (e.g., HSIN-CS);
  - Develop and maintain close working relationships with local (and, as appropriate, Federal, State, tribal, and territorial) law enforcement and first-responder organizations relevant to the company's facilities to promote communication, with the appropriate protections, and cooperation related to prevention, remediation, and response to a natural disaster or terrorist event;
  - Provide applicable information on threats, assets, and vulnerabilities to appropriate government authorities, with the appropriate protections;
  - Share threat and other appropriate information with other CIKR owners and operators;
  - Participate in activities or initiatives developed and sponsored by the relevant NIPP SCC or entity that provides the sector coordinating function;
  - Participate in, share information with (with appropriate protections), and support State and local CIKR protection programs, including coordinating and planning with Local Emergency Planning Committees and Citizen Corps[27] Councils;
  - Collaborate with other CIKR owners and operators on security issues of mutual concern; and
  - Use appropriate measures to safeguard information that could pose a threat and 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, mitigation, and business continuity-of-operations plans;
  - Participate in Federal, State, local, or company exercises and other activities to enhance individual, organization, and sector preparedness and resiliency;
  - Demonstrate a continuous commitment to security and resilience across the entire company;
  - Develop an appropriate security protocol corresponding to each level of the HSAS. 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 or cybersecurity measures in operation at these facilities and modify them as the threat level decreases;
  - Utilize National Fire Protection Association 1600 Standard on Disaster/Emergency Management and Business Continuity Programs, endorsed by DHS and Congress, when developing Emergency Response and Business Continuity-of-Operations Plans if the sector has not developed its own standard;
  - 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 or neighboring facilities;
  - Perform periodic assessments or audits to measure the effectiveness of planned physical security and cybersecurity measures. These audits and verifications should be reported directly to the CEO or his/her designee for review and action;

[27] The U.S. Citizen Corps is the FEMA grassroots strategy to achieve community preparedness and resilience. Local Citizen Corps Councils bring government and civic leaders from all sectors together to develop goals and strategies for community resilience tailored to specific community vulnerabilities and population. Elements of local strategies include: outreach and education on personal preparedness; integration of nongovernmental assets and personnel in preparedness and response protocols; improved plans for emergency notifications, evacuation, and sheltering; and increased citizen participation in community safety. More information is available on the Internet at www.CitizenCorps.gov.

– Promote preparedness education and outreach and emergency response training through the U.S. Citizen Corps, such as the Community Emergency Response Team training offered for employees;

– Consider including programs for developing highly secure and trustworthy operating systems in near-term acquisitions or R&D priorities;

– Participate in the Voluntary Private Sector Preparedness Accreditation and Certification Program, which establishes a common set of criteria for private sector preparedness in disaster management, emergency management, and business continuity;

– Create a culture of preparedness, reaching every level of the organization's workforce, which ingrains in each employee the importance of awareness and empowers those with responsibilities as first-line defenders within the organization and the community;

– As the organization performs R&D or acquires new or upgraded systems, consider only those that are highly secure and trustworthy;

– Encourage employee participation in community preparedness and protection efforts, such as sector-specific Watch programs and skill-based volunteer programs, including Medical Reserve Corps, Red Cross, Second Harvest, etc.;

– Work with others locally, including government, nongovernmental organizations, and private sector entities, both within and outside of the sector, to identify and resolve gaps that could occur in the context of a terrorist incident, natural disaster, or other emergency;

– Work with DHS to improve cooperation regarding personnel screening and information protection; and

– Identify supply chain and "neighbor" issues that could cause workforce or production disruptions for the company.

Appendix 6: S&T Plans, Programs, and Research & Development

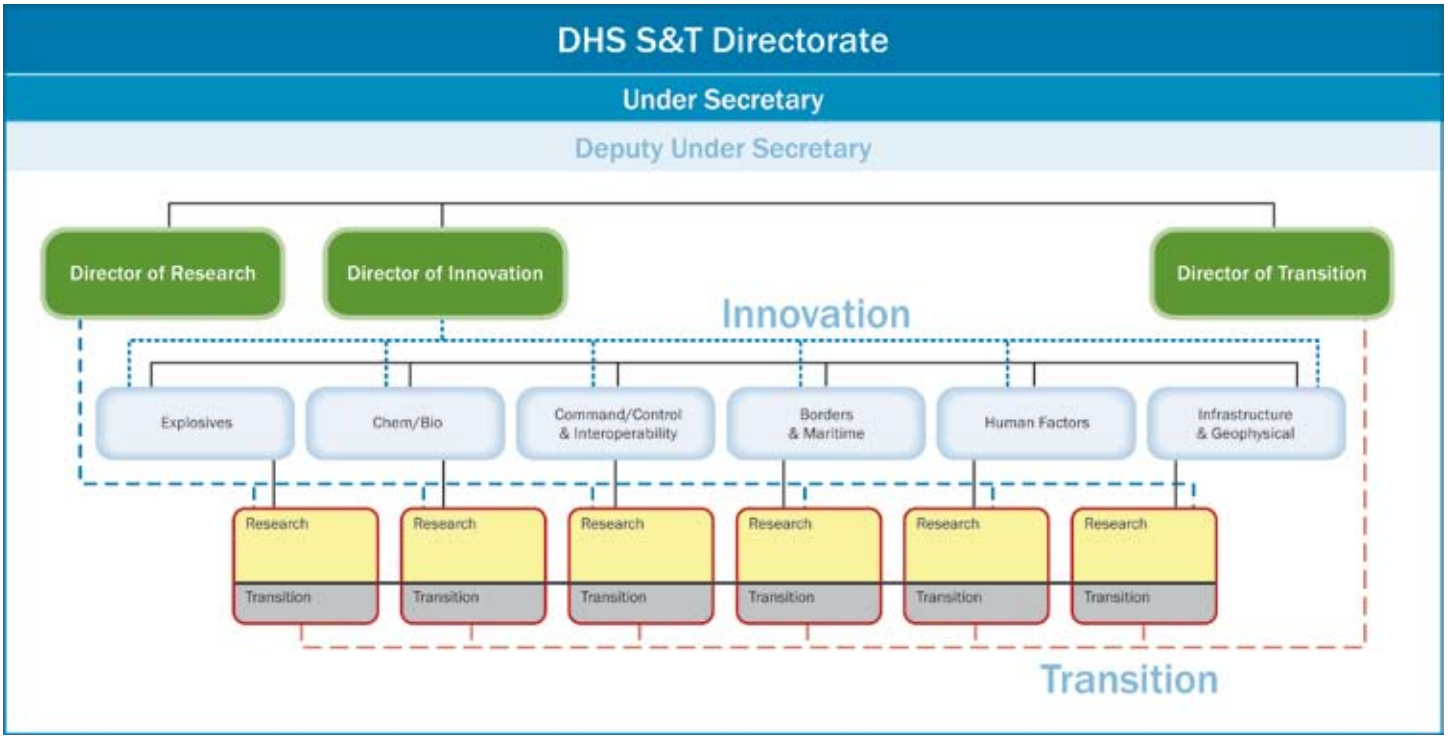
This appendix provides additional details on S&T programs and initiatives supporting the NIPP and CIKR protection. It includes details on how S&T is organized to produce and execute its investment strategy and how that strategy results in developing technology-based solutions to meet customer/end-user requirements.

6.1 S&T Organization and Investment Process

The organization of S&T results in an improved process to identify, validate, and procure new technologies, as well as to develop and integrate technology with the strategies, policies, and procedures required to protect the Nation's CIKR. The division's research, development, test, and evaluation (RDT&E) program achieves S&T strategic goals in six fundamental disciplines: (1) Explosives; (2) Chemical and Biological; (3) Command, Control, and Interoperability; (4) Borders and Maritime Security; (5) Human Factors; and (6) Infrastructure and Geophysical, which also represent S&T's six technical divisions.

These technical divisions are linked to three R&D investment portfolio directors in a "matrix management" structure. These three portfolio directors—the Director of Research, the Director of Transition, and the Director of Innovation/Homeland Security Advanced Research Projects Agency (HSARPA)—provide cross-cutting coordination of their respective elements (or thrusts) of the investment strategy within the technical divisions. Each technical division comprises at least one Section Director of Research who reports to the Director of Research (in addition to the Division Director) so that a cross-cutting focus on basic and applied research capabilities is maintained and leveraged. It also comprises a Section Director of Transition who reports to the Director of Transition (in addition to the Division Director) to help the division stay focused on technology transition.

The Director of Transition coordinates within the department to expedite technology transition and transfer to customers. The Director of Innovation/HSARPA sponsors basic and applied homeland security research to: promote revolutionary changes in technologies; advance the development, testing and evaluation, and deployment of critical homeland security technologies; and accelerate the prototyping and deployment of technologies that would address homeland security vulnerabilities and works



with each of the Division Heads to pursue game-changing, leap-ahead technologies that will significantly lower costs and markedly improve operational capabilities through technology application.

This cross-cutting coordination facilitates a unity of effort. The matrix structure also allows S&T to provide more comprehensive and integrated technology solutions to its customers by appropriately bringing all of the disciplines together in developing solutions.

6.1.1 R&D Investments and Planning

Along with the organizational alignment discussed above, S&T has also aligned its investment portfolio to create an array of programs that balance project risk, cost, mission impact, and the time it takes to deliver solutions. S&T executes projects across the spectrum of technical maturity and transitions them in accordance with customer needs. Its investment portfolio is balanced across long-term research, product applications, and leap-ahead, game-changing capabilities while also meeting mandated requirements. This balanced portfolio ensures that S&T maintains a self-replenishing pipeline of future capabilities and products to transition to customers.

The DHS Transition Program is a formalized, structured process that aligns investments with end-user requirements and is managed by Capstone Integrated Product Teams (IPTs). These teams constitute the Transition portfolio of S&T, targeting deployable capabilities in the near term. S&T established these teams to coordinate the planning and execution of R&D programs together with the eventual hand-off to the maintainers and users of the project results. They are critical nodes in the process for determining operational requirements, assessing current capabilities to meet operational needs, analyzing gaps in capabilities, and articulating programs and projects to fill in the gaps and expand competencies.

IPTs generally include the research and technology perspective, the customer/end-user perspective, and an acquisitions perspective. IPTs are specifically chartered to ensure that technologies are engineered and integrated into systems scheduled for delivery and made available to DHS customers and other homeland security partners. The customers/end-users monitor and guide the capability being developed; the research and technology representatives inform the discussions with scientific and engineering advances and emerging technologies; and the acquisitions staff help transition the results into practice by the maintainers and end-users of the capability.

The IPT topic areas reflect the capability requirements of homeland security stakeholders. The current IPTs operated by S&T are listed below. Each sponsors projects that are relevant to the CIKR protection mission. The three bolded IPTs are chaired or co-chaired by IP.

Information Sharing/Management	**Counter IED**
Border Security	Cargo Security
Chem/Bio Defense	People Screening
Maritime Security	**Infrastructure Protection**
Cyber Security	Preparedness & Response: Incident Management
Transportation Security	Preparedness & Response: Interoperability

Each IPT identifies, validates, and prioritizes requirements for S&T and provides critical input to investments in programs and projects that will ultimately deliver technology solutions that can be developed, matured, and delivered to customer acquisitions programs for deployment in the field. Investments are competitively selected and focus on DHS's highest-priority, risk-based requirements that provide capabilities to customers/end-users. A successful transition portfolio requires sustained customer feedback from DHS components to ensure that programs address genuine capability gaps. To gain this insight, S&T established 46 Project IPTs and semi-annually reaches out to DHS components to gauge their overall satisfaction with delivered products and capabilities. The results are explicitly tied to the outcome-based performance metrics of cost, schedule, and technology readiness.

6.2 Requirements

S&T's programs are motivated by the requirements of the DHS operating components and other homeland security partners. For CIKR protection, requirements are developed by the SSAs and their private sector and government partners. The National Risk Profile drives sector requirements, as well as the cross-sector prioritization of requirements. Prioritized requirements are, in turn, the basis for the NCIP R&D Plan, which advises investments across the Federal R&D community.

CIKR protection requirements have led to several initiatives and actions necessary for NIPP implementation, particularly regarding initiatives to:

- Review and revise CIKR-related plans, as needed, to reinforce the linkage between NIPP steady-state CIKR protection and NRF incident management requirements;
- Identify cross-sector vulnerabilities; and
- Communicate requirements for CIKR-related R&D to DHS for use in the national R&D planning effort.

6.2.1 High-Priority Technology Needs

Each year, S&T publishes the high-priority technology needs in its specified functional areas. The following is a representative sample of needs for the Nation's CIKR:

- Analytical tools to quantify interdependencies and cascading consequences as disruptions occur across critical infrastructure sectors;
- Effective and affordable blast analysis and protection for critical infrastructure and an improved understanding of blast-failure mechanisms and protection measures for the most vital CIKR;
- Advanced, automated, and affordable monitoring and surveillance technologies, specifically, decision support systems to prevent disruption, mitigate results, and build resiliency;

- Rapid mitigation and recovery technologies to quickly reduce the effects of natural and manmade disruptions and cascading effects; and
- Critical utility components that are affordable and highly transportable, and provide robust solutions during manmade and natural disruptions.

6.2.2 Industry Involvement

Industry is a valued partner of S&T. Its continued participation in developing solutions for homeland security applications is vital to our effort to safeguard the Nation. Consistent with the directorate's new structure, the Innovation/HSARPA portfolio and six technical divisions will proactively seek industry participation to address specific challenges in their respective areas. Additionally, private sector owners and operators, through the SCCs, have provided powerful independent validation of the R&D priorities set by the Federal CIKR community. Several GCCs and SCCs have established joint R&D working groups to provide course-correcting input for future R&D direction.

6.3 Executing R&D Programs

Critical infrastructure is a widely distributed enterprise across multiple industries, government agencies, and academia, so its R&D program cannot be managed through a command and control-type process. Instead, DHS and OSTP are fostering an evolving network of partnerships and coordination groups. These groups have different focuses, including sector-specific needs, technology themes of interest to multiple sectors, and committees that coordinate Federal agency resources. The requirements process, translated into investment priorities, provides the goals and plans that allow this distributed R&D enterprise to act in coordinated ways. The National Annual Report and the NCIP R&D Plan communicate this overarching R&D strategy and help identify which R&D requirements are best met by the private versus the public sector.

6.3.1 Partnerships and Collaboration

The NIPP Partnership Framework

The CIPAC, established by DHS, has been very effective in helping Federal infrastructure protection groups work with the private sector and with State, local, tribal, and territorial governments. The CIPAC provides a forum in which the sectors have engaged very actively in a broad spectrum of activities to implement their sector protection plans, including planning, prioritizing, and coordinating R&D agendas.

Sector and Cross-Sector Coordination

The Sector R&D Working Groups, typically Joint SCC and GCC, have developed well-founded technical R&D agendas that are essential for their sector in order to achieve sector security goals. These R&D agendas coordinate challenges across the spectrum of sector stakeholders and are used to represent sector R&D interests in cross-sector settings. The executive managers of each sector coordinate activities through the FSLC. The SCCs have formed a cross-sector group, the CIKR Cross-Sector Council,[28] to coordinate cross-sector initiatives that promote public and private infrastructure protection initiatives. One of the objectives of the CIKR Cross-Sector Council is to provide cross-sector input regarding R&D priorities; this input is informed by the results of risk assessments in each sector, as well as the National Risk Profile.

Universities

Universities and research centers across multiple Federal agencies contribute to agency mission accomplishment and CIKR protection from the time before a disruptive event to the time after a disruptive event. The DHS Centers of Excellence contribute to the national-level implementation of the NIPP and to CIKR protection; their contributions take different forms, including the following:

[28] The CIKR Cross-Sector Council comprises the leadership of each of the SCCs; the Partnership for Critical Infrastructure Security currently provides this representation.

- Provide independent analysis of CIKR protection (full-spectrum) issues;
- Conduct research and provide innovative perspectives on threats and the behavioral aspects of terrorism;
- Conduct research to identify new technologies and analytical methods that can be applied by CIKR partners to support NIPP efforts;
- Support research, development, testing, evaluation, and deployment of CIKR protection technologies;
- Analyze, provide, and share best practices related to CIKR protection efforts; and
- Develop and provide suitable security risk analysis and risk management courses for CIKR protection professionals.

International

DHS, DoD, DOE, and other Federal agencies have undertaken many different outreach efforts to foreign government representatives and organizations that are pursuing similar R&D planning and performance. Agreements of cooperation, joint pursuit, and knowledge sharing have been created with France, Germany, Japan, Israel, Italy, the Netherlands, Russia, the Scandinavian countries, the United Kingdom, and others. Other organizations, such as the TSWG, also have developed successful R&D collaborations with a number of countries.

State and Local

State, local, tribal, and territorial governments play an important role in the protection of the Nation's CIKR. These governmental entities not only have CIKR under their direct control, but also have CIKR owned and operated by other partners who are within their jurisdictions. The SLTTGCC and RCCC bring national CIKR protection principles to the State, local, and regional levels and are important sources of capability requirements that drive R&D priorities.

Industry Organizations

In addition to R&D input provided by government organizations, there are major industrial groups that provide input and comment in order to influence future R&D by illuminating issues that they have encountered and issues that are likely based on new product development that they are doing but cannot discuss openly for competitive reasons. For example, the INFOSEC Research Council has provided valuable input on cybersecurity, including the publication of a Hard Problems List[29] that is an important planning tool used by all R&D contributors. The NSTAC identified critical gaps that require new cyber and telecommunications R&D.

6.4 Five-Year Strategy/Technology Roadmap

S&T implements its business approach through its Planning, Programming, Budgeting, and Execution (PPBE) process, which encompasses the development of priorities, program plans, resource requirements, and associated performance metrics. The PPBE process builds the framework to link strategy for the out-years to program execution in the present. It ensures that the directorate remains mission-focused, customer-oriented, and threat- and risk-informed in order to prioritize resource allocation and remain accountable in its efforts to secure the homeland.

The 5-year execution plan: details the S&T investment portfolio; outlines the directorate's activities and plans at the division level; and includes each division's research thrusts, programs, and key milestones. It supports the department's strategic plan and priorities, as well as S&T's priorities. The 5-year plan is the roadmap for achieving success; however, the planning process must be flexible in order to adjust to a changing homeland security environment. The plan will be updated annually to ensure that it continues to address the correct set of priorities, fills customers' homeland security capability gaps, and enables the achievement of a safer homeland.

[29] See http://www.cyber.st.dhs.gov/docs/IRC_Hard_Problem_List.pdf.

Homeland Security