2. Authorities, Roles, and Responsibilities

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

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

2.1 Authorities

The roles and responsibilities described in this chapter are derived from a series of authorities, including the Homeland Security Act of 2002, other CI/KR protection-related legislation, executive orders, Homeland Security Presidential directives, and Presidential strategies. The National Strategy for Homeland Security established the national CI/KR vision with a charge to "forge an unprecedented level of cooperation throughout all levels of government, with private industry and institutions, and with the American people to protect our critical infrastructures and key assets from terrorist attack."[11] HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection, provided the direction to implement this vision. More detailed information on these and other CI/KR protection-related authorities is included in 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 CI/KR. It established the DHS mission, including "reducing the Nation's vulnerability to terrorist attacks," major disasters, and other emergencies, and charged the department with the responsibility for evaluating vulnerabilities and ensuring that steps are implemented to protect the high-risk elements of America's CI/KR, including food and water systems, agriculture, health systems and emergency services, information technology, telecommunications, 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

[11] The National Strategy for Homeland Security uses the term "key assets," defined as individual targets whose destruction would not endanger vital systems, but could create local disaster or profoundly damage 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.

the act assigned primary responsibility to DHS to develop a comprehensive national plan for securing CI/KR and for recommending "the measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other agencies of the Federal Government and in cooperation with State and local government agencies and authorities, the private sector, and other entities."

A number of other statutes provide authorities both for cross-sector and sector-specific CI/KR protection efforts. Some examples of other CI/KR protection-related legislation include: The Public Health Security and Bioterrorism Preparedness and Response Act of 2002, which was intended to improve the ability of the United States to prevent, prepare for, and respond to acts of bioterrorism and other public health emergencies; the Maritime Transportation Security Act; the Energy Policy and Conservation Act; the Critical Infrastructure Information Act; the Federal Information Security Management Act; and various others.

These separate authorities are tied together as part of the national approach for CI/KR protection through the unifying framework established in HSPD-7. HSPD-7, issued in December 2003, established the U.S. policy for "enhancing protection of the Nation's CI/KR." HSPD-7 establishes a framework for security partners to identify, prioritize, and protect the Nation's CI/KR 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, and tribal governments; the private sector; and other security partners. The following sections address security partner 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 national-level impact, it is incumbent upon the Federal Government to provide overarching leadership and coordination in the CI/KR protection mission area.

2.2.1 Department of Homeland Security

Under HSPD-7, DHS is responsible for leading, integrating, and coordinating the overall national effort to enhance CI/KR protection, including collaborative development of 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 uniform security practices and harmonizing security 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 CI/KR protection program.

In addition to these overarching leadership and cross-sector responsibilities, DHS serves as the SSA for 10 of the CI/KR sectors identified in HSPD-7: Information Technology; Telecommunications; Transportation; Chemical; Emergency Services; Commercial Nuclear Reactors, Material, and Waste; Postal and Shipping; Dams; Government Facilities; and Commercial Facilities. Specific SSA responsibilities are discussed in section 2.2.2.

Additional DHS CI/KR 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 CI/KR 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 security partnerships and leveraging sector-specific security expertise, relationships, and resources across CI/KR sectors, including oversight and support of the sector partnership model described in chapter 4; cooperation with Federal, State, local, and tribal security partners; and collaborating with the Department of State to reach out to foreign countries and international organizations to strengthen the protection of U.S. CI/KR;
- 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 security

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 CI/KR vulnerabilities;
- Coordinating, facilitating, and supporting comprehensive risk assessment programs for high-risk CI/KR, identifying protection priorities across sectors and jurisdictions, and integrating CI/KR protective programs with the all-hazards approach to domestic incident management described in HSPD-5;
- Facilitating the sharing of CI/KR protection best practices and processes, and risk assessment methodologies and tools across sectors and jurisdictions;
- Sponsoring CI/KR protection-related research and development (R&D), demonstration projects, and pilot programs;
- Seeding development and transfer of advanced technologies while leveraging private sector expertise and competencies, including participation in the development of voluntary consensus standards or best practices as appropriate;
- Promoting national-level CI/KR protection education, training, and awareness in cooperation with State, local, tribal, and private sector partners;
- Identifying and implementing plans and processes for step-ups in protective measures that align to all-hazards warnings, specific threat vectors 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 security partners, as appropriate;
- Informing the annual Federal budget process based on CI/KR risk and need in coordination with SSAs and other security partners;
- Monitoring performance measures for the national CI/KR protection program and NIPP implementation process to enable continuous improvement, and providing annual CI/KR protection reports to the Executive Office of the President that include current status, priorities, progress, and gaps in program authorities or resources, and recommended corrective actions;
- Integrating national efforts for the protection and recovery of critical information systems and cyber components of physical CI/KR, including analysis, warning, information-sharing, vulnerability reduction, and mitigation activities and programs;
- Evaluating preparedness for CI/KR protection across sectors and jurisdictions as a component of the National Exercise Program;
- Documenting lessons learned from exercises, actual incidents, and pre-disaster mitigation efforts, and applying those lessons, where applicable, to CI/KR protection efforts;
- Working with the Department of State, SSAs, and other security partners to ensure that U.S. CI/KR protection efforts are fully coordinated with international partners; and
- Evaluating the need for and coordinating the protection of additional CI/KR categories over time, as appropriate.

2.2.2 Sector-Specific Agencies

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

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

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

Sector-Specific Agency	Critical Infrastructure/Key Resources Sector
Department of Agriculture[12] Department of Health and Human Services[13]	Agriculture and Food
Department of Defense[14]	Defense Industrial Base
Department of Energy	Energy[15]
Department of Health and Human Services	Public Health and Healthcare
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Drinking Water and Water Treatment Systems
Department of Homeland Security *Office of Infrastructure Protection*	Chemical Commercial Facilities Dams Emergency Services Commercial Nuclear Reactors, Materials, and Waste
Office of Cyber Security and Telecommunications	Information Technology Telecommunications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration, United States Coast Guard[16]	Transportation Systems[17]
Immigration and Customs Enforcement, Federal Protective Service	Government Facilities

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

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

[14] 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.

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

[16] The U.S. Coast Guard (USCG) is the SSA for the maritime transportation mode.

[17] 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.

SSAs perform the activities above, as appropriate and consistent with existing authorities (including regulatory authorities in some instances), in close cooperation with other security partners. HSPD-7 requires SSAs to provide an annual report to the Secretary of Homeland Security on their efforts to identify, prioritize, and coordinate CI/KR protection in their respective sectors. Consistent with this requirement, DHS will provide reporting guidance and templates that include requests for specific information, such as sector CI/KR protection priorities, requirements, and resources. SSAs also are responsible for outlining these sector-specific CI/KR protection requirements and related budget projections as a component of their annual budget submissions to the Office of Management and Budget (OMB).

Additional SSA responsibilities include:

- Identifying, prioritizing, and coordinating the protection of sector-level CI/KR with a particular focus on CI/KR that could be exploited to cause catastrophic health effects or mass casualties comparable to those produced by a WMD;
- Managing the overall process for building security partnerships and leveraging CI/KR 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 CI/KR, identifying protection priorities, and incorporating CI/KR 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 CI/KR protection best practices and processes, and risk assessment methodologies and tools within the sector;
- Promoting sector-level CI/KR protection education, training, and awareness in coordination with State, local, tribal, and private sector partners;
- Informing the annual Federal budget process based on CI/KR risk and protection needs in coordination with security partners and allocating resources for CI/KR protection accordingly;
- Monitoring performance measures for sector-level CI/KR protection and NIPP implementation activities 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;
- Supporting DHS-initiated data calls to populate the National Asset Database (NADB), enable national-level risk assessment, and inform national-level resource allocation;
- Supporting protocols for the Protected Critical Infrastructure Information (PCII) Program;
- Working with DHS to develop, evaluate, validate, or modify sector-specific risk assessment tools;
- Supporting sector-level dependency, interdependency, consequence, and other analysis as required;
- Coordinating sector-level participation in the National Exercise Program, Homeland Security Exercise and Evaluation Program (HSEEP), and other sector-level activities;
- Assisting sector security 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 CI/KR protection practices and methodologies;
- Identifying and implementing plans and processes for step-ups in protective measures that align to all-hazards warnings, specific threat vectors 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
- Supporting DHS and Department of State efforts to integrate U.S. CI/KR protection programs into the international and global markets, and address relevant dependency, interdependency, and cross-border issues.

2.2.3 Other Federal Departments, Agencies, and Offices

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

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

- Assist in assessing risk, prioritizing CI/KR, and enabling protective actions and programs within that sector;
- Support the national goal of enhancing CI/KR protection through their roles as the regulatory agencies for owners and operators represented within specific sectors when so designated by statute; and
- Collaborate with all relevant security partners to share security-related information within the sector, as appropriate.

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

Under HSPD-7, a number of Federal departments and agencies and components of the Executive Office of the President have special functions related to CI/KR 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 Department of State**, in coordination with DHS and the Departments of Justice (DOJ), Commerce, Defense, and Treasury, works with foreign governments and international organizations to strengthen U.S. CI/KR protection efforts.
- **The Department of Justice**, including the Federal Bureau of Investigation (FBI), acts to reduce terrorist threats, and investigates and prosecutes actual or attempted attacks on, sabotage of, or disruptions of CI/KR in collaboration with DHS.
- **The Department of Commerce** 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 industrial products, materials, and services 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 additionally 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 nuclear materials and waste. In addition, the NRC collaborates with DHS on any changes in the protective measures for this sector.
- **The Intelligence Community, the Department of Defense, and other appropriate Federal departments**, such as the Department of the Interior and DOT, are collaborating with DHS on the development and implementation of a geospatial program to map, image, analyze, and sort CI/KR 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 CI/KR sectors such as Banking and Finance and Telecommunications. 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 CI/KR protection based on advice from the Critical Infrastructure Protection Policy Coordinating Committee (PCC). This PCC is chaired by a Federal officer or employee designated by the Assistant to the President for Homeland Security.
- **The Office of Science and Technology Policy** coordinates with DHS to further interagency R&D related to CI/KR protection.
- **The Office of Management and Budget** oversees the implementation of government-wide policies, principles, standards, and guidelines for Federal Government computer security programs.

2.2.4 State, Local, and Tribal Governments

State, local, and tribal 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 the protection of the Nation's CI/KR, including CI/KR under their control, as well as CI/KR owned and operated by other NIPP security 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 plans. They are equally critical in terms of enabling time-sensitive, post-event CI/KR response, restoration, and recovery activities.

Security partners at all levels of government have recently developed homeland security strategies that align with and support the priorities established in the National Preparedness Goal. With the inclusion of NIPP implementation as one of these national priorities, CI/KR protection programs form an essential component of State, local, and tribal 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, including key cross-jurisdictional security and information-sharing linkages, as well as specific CI/KR protective programs focused on risk management. These programs play a primary role in the identification and protection of CI/KR locally and also support DHS and SSA efforts to identify, ensure connectivity with, and enable the protection of CI/KR of national-level criticality within the jurisdiction.

2.2.4.1 State and Territorial Governments

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

State governments are responsible for developing and implementing statewide/regional CI/KR protection programs that reflect the full range of NIPP-related activities. State programs should address all relevant aspects of CI/KR 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 CI/KR protection efforts should be integrated into the overarching homeland security program framework at the State level to ensure that prevention, protection, response, and recovery efforts are synchronized and mutually supportive. CI/KR protection at the State level must cut across all sectors present within the State and support national, State, and local priorities. The program also should explicitly address unique geographical issues, including trans-border concerns, as well as interdependencies among sectors and jurisdictions within those geographical boundaries.

Specific CI/KR protection-related activities include:

- Acting as a focal point for and promoting the coordination of protective and emergency response activities, preparedness programs, and resource support among local jurisdictions and regional partners;
- Developing a unified approach to CI/KR 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 private entities resident within them;
- Facilitating the exchange of security information, including threat assessments, attack indications and warnings, and advisories, within and across jurisdictions and sectors therein;
- Participating in the NIPP sector partnership model, including Government Coordinating Councils (GCCs), Sector Coordinating Councils (SCCs), and other CI/KR governance efforts and SSP planning efforts relevant to the given jurisdiction;
- Ensuring that funding priorities are addressed and that resources are allocated efficiently and effectively to achieve the CI/KR protection mission in accordance with relevant plans and strategies;
- Sharing information on CI/KR deemed critical from national, State, regional, local, and/or tribal perspectives to enable prioritized protection and restoration of critical public services, facilities, utilities, and processes within the jurisdiction;
- Addressing unique geographical issues, including trans-border concerns, dependencies, and interdependencies among the sectors within the jurisdiction;
- Identifying and implementing plans and processes for step-ups in protective measures that align to all-hazards warnings, specific threat vectors 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 CI/KR protection context;
- Identifying and communicating requirements for CI/KR-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 CI/KR-related funding projections.

2.2.4.2 Local Governments

Local governments represent the front lines for homeland security and, more specifically, for CI/KR 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 government entities own and operate CI/KR such as water, stormwater, and electric utilities. Most disruptions or malevolent acts that impact CI/KR 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 security partners, including government agencies, owners and operators, and private citizens in the communities they serve.

CI/KR 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 unified approach at the local level to CI/KR identification, risk determination, mitigation planning, and prioritized security investment, and exercising preparedness among all relevant security partners within the jurisdiction;
- 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;
- Facilitating the exchange of security information, including threat assessments, attack indications and warnings, and advisories, among security partners within the jurisdiction;
- Participating in the NIPP sector partnership model, including GCCs, SCCs, and other CI/KR governance efforts and SSP planning efforts relevant to the given jurisdiction;
- Ensuring that funding priorities are addressed and that resources are allocated efficiently and effectively to achieve

the CI/KR protection mission in accordance with relevant plans and strategies;

- Sharing information with security partners, as appropriate, on CI/KR deemed critical from the local perspective to enable prioritized protection and restoration of critical public services, facilities, utilities, and processes within the jurisdiction;
- Addressing unique geographical issues, including trans-border concerns, dependencies, and interdependencies among agencies and enterprises within the jurisdiction;
- Identifying and implementing plans and processes for step-ups in protective measures that align to all-hazards warnings, specific threat vectors 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 CI/KR protection context; and
- Conducting CI/KR protection public awareness activities.

2.2.4.3 Tribal Governments

Tribal government roles and responsibilities regarding CI/KR 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 CI/KR and continuity of essential services under their jurisdiction. Under the NIPP partnership model, tribal governments must ensure close 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, protective program investments and initiatives, and resource allocation. To facilitate this interaction, tribal governments, as appropriate, should be active participants in the NIPP governance structures detailed in chapter 4.

2.2.4.4 Regional Partners

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

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

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

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

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 CI/KR 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 SSAs within a State and contribute expertise, assist with regulatory authorities, or help to facilitate investment decisions related to CI/KR protection efforts within a given jurisdiction or geographical region.

2.2.5 Private Sector Owners and Operators

Owners and operators generally represent the first line of defense for the CI/KR under their control. Private sector owners and operators are responsible for taking action to support risk management planning and investments in security as a necessary component of prudent business planning and operations. In today's risk environment, these activities generally include reassessing and adjusting continuity-of-business and emergency management plans, building increased resiliency and redundancy into business processes and systems, protecting facilities against physical and cyber attacks and natural disasters, guarding against the insider threat, and increasing coordination with external organizations to avoid or minimize the impacts 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 in an environment of limited resources. In the context of the first factor, the Federal Government is uniquely postured to help inform critical security investment decisions and operational planning. For example, owners and operators generally look to the government as a source of security-related best practices and for attack indications, warnings, and threat assessments. In relationship to the second factor, owners and operators also generally rely on government entities to address risks outside of their property or in situations in which the current threat exceeds an enterprise's capability to protect itself or mitigate risk beyond a reasonable level of additional investment. In this situation, public and private sector security partners at all levels must collaborate to address the protection of national-level CI/KR, provide timely warning, and promote an environment in which CI/KR owners and operators can better carry out their specific protection responsibilities. Additionally, CI/KR owners and operators may be required to invest in security as a result of Federal, State, and/or local regulations.

The CI/KR protection responsibilities of specific owners or operators vary widely within and across sectors. Some sectors have regulatory or statutory frameworks that govern private sector security operations within the sector; however, most are guided by voluntary security regimes or adherence to

Public Utility Commissions provide an example of a State entity with responsibility for electricity, gas, and telecommunications infrastructures and, in some cases, water, wastewater/sewage, and certain aspects of transportation. As such, Public Utility Commissions are uniquely positioned to deal with the recovery of investments made for protection of critical infrastructure in these areas. Furthermore, Public Utility Commissions historically have been concerned with the adequacy and reliability of these services, and have facilitated investments made by these industries to ensure that they are resilient and reliable.

For example, Public Utility Commissions work together to address issues of mutual concern based on the interdependencies between the water, telecommunications, and energy infrastructures (in the context of preparedness for, and response to, events impacting critical infrastructure) by:

- Creating networks among utility regulators and other Federal, State, local, and private sector entities to address cross-sector issues;
- Exploring and recommending solutions for information disclosure issues (especially protecting sensitive security information from public disclosure while ensuring that all critical stakeholders have access to essential information);
- Exploring and recommending solutions to cost-recovery issues associated with key water, gas, telecommunications, and energy infrastructures; and
- Identifying and prioritizing issues, researching best practices, and disseminating information to Federal and State partners and affiliates.

industry-promoted best practices. Within this diverse protective landscape, private sector entities can better secure the CI/KR under their control by:

- Performing comprehensive risk assessments tailored to their specific sector, enterprise, or facility risk landscape;
- Developing an awareness of critical dependencies and interdependencies at the sector, enterprise, and facility levels;
- Implementing protective actions and programs to reduce identified vulnerabilities appropriate to the level of risk presented;
- Establishing cyber security programs and associated awareness training within the organization;
- Adhering to recognized industry best business practices and standards, including those with a cyber security nexus (see appendix 5B);
- Developing and coordinating CI/KR protective and emergency response actions, plans, and programs with appropriate Federal, State, and local government authorities;
- Participating in the NIPP sector partnership model (including SCCs and information-sharing mechanisms), as appropriate;
- Assisting and supporting Federal, State, local, and tribal government CI/KR data collection and protection efforts, as appropriate;
- 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 where appropriate;
- Promoting CI/KR protection education, training, and awareness programs;
- Adopting and implementing effective workforce security assurance programs to mitigate potential insider threats;
- Providing technical expertise to SSAs and DHS when appropriate;
- Participating in regular CI/KR protection-focused exercise programs with other public and private sector security partners;
- Identifying and communicating requirements to DHS and/or SSAs for CI/KR 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 help remove barriers to public-private partnerships.

2.2.6 Advisory Councils

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

- Critical Infrastructure Partnership Advisory Council (CIPAC): CIPAC is a partnership between government and private sector CI/KR owners and operators that facilitates effective coordination of Federal CI/KR protection programs. CIPAC engages in a range of CI/KR protection activities such as planning, coordination, NIPP implementation, and operational activities, including incident response, recovery, and reconstitution. DHS published a Federal Register Notice on March 24, 2006, announcing the establishment of CIPAC as a Federal Advisory Committee Act (FACA)[18]-exempt body pursuant to section 871 of the Homeland Security Act (see chapter 4).
- Homeland Security Advisory Council (HSAC): The HSAC provides advice and recommendations to the Secretary of Homeland Security on relevant issues. The Council members, appointed by the DHS Secretary, include experts from State and local 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 the PVTSAC as a subcommittee of the HSAC to provide the HSAC with expert advice from leaders in the private sector.

[18] 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 which could prevent a meeting on short notice to discuss sensitive information in an appropriate setting.

- National Infrastructure Advisory Council (NIAC): The NIAC provides the President, through the Secretary of Homeland Security, with advice on the security of physical and cyber systems across all CI/KR sectors. The Council is comprised of 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): The NSTAC provides industry-based advice and expertise to the President on issues and problems related to implementing National Security and Emergency Preparedness (NS/EP) communications policy. The NSTAC is comprised of up to 30 industry chief executives representing the major communications and network service providers and information technology, finance, and aerospace companies. It was created under Executive Order 12382.

2.2.7 Academia and Research Centers

The academic and research center communities play an important role in enabling national-level CI/KR 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 CI/KR protection issues;
- Supporting the research, development, testing, evaluation, and deployment of CI/KR protection technologies;
- Analyzing, developing, and sharing best practices related to CI/KR protection efforts;
- Researching and providing innovative thinking and perspective on threats and the behavioral aspects of terrorism;
- Preparing or disseminating guidelines, courses, and descriptions of best practices for physical security and cyber security;
- Developing and providing suitable security risk analysis and risk management courses for CI/KR protection professionals; and
- Conducting research to identify new technologies and analytical methods that can be applied by security partners to support NIPP efforts.