

4. Organizing and Partnering for CI/KR Protection

The enormity and complexity of the Nation's CI/KR, the distributed character of its associated protective architecture, and the uncertain nature of the terrorist threat and manmade or natural disasters make the effective implementation of protection 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 CI/KR protection efforts at the Federal, State, regional, local, tribal, and international levels, as well as between public and private sector security partners. In addition to direct coordination between security partners, the structures described below provide a national framework that fosters relationships and facilitates coordination within and across CI/KR sectors:

- **National-Level Coordination:** The DHS Office of Infrastructure Protection (OIP) facilitates overall development of the NIPP and SSPs, provides overarching guidance, and monitors the full range of associated coordination activities and performance metrics.
- **Sector Partnership Coordination:** The Private Sector Cross-Sector Council (i.e., the Partnership for Critical Infrastructure Security (PCIS)), the Government Cross-Sector Council (made up of two subcouncils: the NIPP Federal Senior Leadership Council (FSLC) and the State, Local, and Tribal Government Coordinating Council (SLTGCC)), 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 CI/KR protection.
- **Regional Coordination:** Regional partnerships, groupings, and governance bodies enable CI/KR protection coordination among security partners within and across geographical areas and sectors. Such bodies are composed of representatives from industry and State, local, and tribal entities located in whole or in part within the planning area for an aggregation of high-risk targets, urban areas, or cross-sector groupings. They facilitate enhanced coordination between jurisdictions within a State where CI/KR cross multiple jurisdictions, and help sectors coordinate with multiple States that rely on a common set of CI/KR. They also are organized to address common approaches to a wide variety of natural or manmade hazards.
- **International Coordination:** The United States-Canada-Mexico Security and Prosperity Partnership; the North Atlantic Treaty Organization's (NATO's) Senior Civil Emergency Planning Committee; certain government councils, such as the Committee on Foreign Investment in

the United States (CFIUS); and consensus-based nongovernmental or public-private organizations, such as the global Forum of Incident Response and Security Teams (FIRST), enable a range of CI/KR protection coordination activities associated with established international agreements.

4.1.1 National-Level Coordination

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

- Leads, integrates, and coordinates the execution of the NIPP, in part by acting as a central clearinghouse for the information-sharing and coordination activities of the individual sector governance structures;
- Facilitates the development and ongoing support of these security partner governance 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 SSAs and other security partners to carry out NIPP responsibilities;
- Facilitates the sharing of CI/KR protection-related best practices and lessons learned;
- Facilitates security partner participation in preparedness activities, planning, readiness exercises, and public awareness efforts; and
- Ensures cross-sector coordination of SSPs to avoid duplicative requirements and reporting, and conflicting guidance.

4.1.2 Sector Partnership Coordination

The goal of these organizational structures, partnerships, and information-sharing networks is to establish the context, framework, and support for activities required to implement and sustain the national CI/KR protection effort. DHS will issue coordinated guidance on the framework for CI/KR public-private partnerships, as well as metrics to measure their effectiveness.

The NIPP relies on the sector partnership model, illustrated in figure 4-1, as the primary organizational structure for coordinating CI/KR efforts and activities. The sector 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 CI/KR protection within and across sectors.

4.1.2.1 Private Sector Cross-Sector Council

Cross-sector issues and interdependencies between the SCCs will be addressed through a Private Sector Cross-Sector Council (i.e., the PCIS):

- **Partnership for Critical Infrastructure Security:** The PCIS membership is comprised of one or more members and their alternates from each of the SCCs. The partnership coordinates cross-sector initiatives to support CI/KR protection by identifying legislative issues that affect such initiatives and by raising awareness of issues in CI/KR protection. The primary activities of the PCIS include:
 - Providing senior-level, cross-sector strategic coordination through partnership with DHS and the SSAs;
 - Identifying and disseminating CI/KR protection best practices across the sectors;
 - Participating in coordinated planning efforts related to the development, implementation, and revision of the NIPP Base Plan and SSPs; and
 - Coordinating with DHS to support efforts to plan and execute the Nation’s CI/KR 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 is comprised of two subcouncils: the NIPP FSLC and the SLTGCC:

- **NIPP Federal Senior Leadership Council:** The objective of the NIPP FSLC is to drive 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 CI/KR risk management strategies;
 - Evaluating and promoting implementation of risk management-based CI/KR protection programs;
 - Advancing CI/KR protection collaboration within and across sectors;
 - Advancing CI/KR protection collaboration with the international community; and

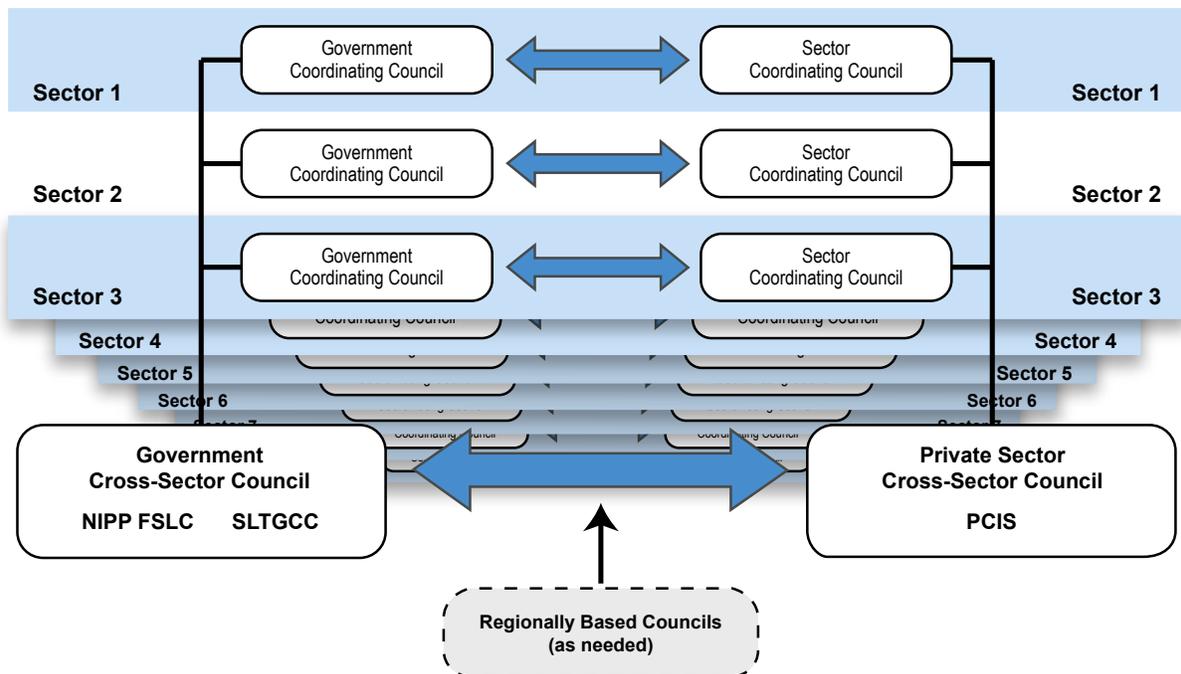
- Evaluating and reporting on the progress of Federal CI/KR protection activities.
- **State, Local, and Tribal Government Coordinating Council:** The SLTGCC serves as a forum to ensure that State, local, and tribal homeland security advisors or their designated representatives are fully integrated as active participants in national CI/KR protection efforts and to provide an organizational structure to coordinate across jurisdictions on State- and local-level CI/KR protection guidance, strategies, and programs. The SLTGCC will provide the State, local, or tribal perspective or feedback on a wide variety of CI/KR issues. The primary functions of the SLTGCC include the following:
 - Providing senior-level, cross-jurisdictional strategic communications and coordination through partnership with DHS, the SSAs, and private sector owners and operators;
 - Participating in planning efforts related to the development, implementation, update, and revision of the NIPP Base Plan and SSPs;
 - Coordinating strategic issues and issue management resolution among State, local, and tribal security partners;
 - Coordinating with DHS to support efforts to plan, implement, and execute the Nation’s CI/KR protection mission; and

- Providing DHS with information on State-, local-, and tribal-level CI/KR 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 CI/KR 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, supporting Federal departments and agencies, and other public and private sector security partners;
- Identify issues shared by multiple sectors that would benefit from common investigations and/or solutions;
- Identify and promote best practices from individual sectors that have applicability to other sectors;
- Contribute to cross-sector planning and prioritization efforts, as appropriate; and
- Provide input to the government on R&D efforts that would benefit multiple sectors.

Figure 4-1: Sector Partnership Model



4.1.2.3 Sector Coordinating Councils

The sector partnership model encourages CI/KR owners and operators to create or identify an SCC as the principal entity for coordinating with the government on a wide range of CI/KR protection activities and issues. SCCs should be self-organized, self-run, and self-governed, with a spokesperson designated by the sector membership. Specific membership will vary 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. 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 CI/KR protection activities and issues for that sector;
- Serve as a strategic communications and coordination mechanism between CI/KR owners, operators, and suppliers, and with the government during response and recovery as determined by the sector;
- Identify, implement, and support the information-sharing capabilities and mechanisms that are most appropriate for the sector. ISACs may perform this role if so designated by the SCC;
- Facilitate inclusive organization and coordination of the sector's policy development regarding CI/KR protection planning and preparedness, exercises and training, public awareness, and associated plan implementation activities and requirements;
- Advise on integration of Federal, State, regional, and local planning with private sector initiatives; and
- Provide input to the government on sector R&D efforts and requirements.

SCCs are encouraged to participate in voluntary consensus standards development efforts to ensure that sector perspectives are included in standards that affect CI/KR protection.²⁰

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 is comprised of representatives across various levels of government (Federal, State, local, or tribal) as appropriate to the security landscape of each individual sector. Each GCC is 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 government 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 Federal departments and agencies;
- Participate in planning efforts related to the development, implementation, update, and revision of the NIPP Base Plan and SSPs;
- Coordinate strategic communications, and issue management and resolution among government entities within the sector; and
- Coordinate with and support the efforts of the SCC to plan, implement, and execute the Nation's CI/KR protection mission.

4.1.2.5 Critical Infrastructure Partnership Advisory Council

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

- Planning, coordination, implementation, and operational issues;

²⁰ 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, though 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, government-unique standards developed by government for its own uses, and standards mandated by law.

- Implementation of security programs;
- Operational activities related to CI/KR protection, including incident response, recovery, and reconstitution; and
- Development and support of national plans, including the NIPP and the SSPs.

The CIPAC membership consists of private sector CI/KR 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 government entities (including their representative trade or equivalent associations) that comprise 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 CI/KR protection coordination among security 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 to address cross-sector CI/KR planning and protection program implementation. They may also provide enhanced coordination between jurisdictions within a State where CI/KR cross multiple jurisdictions and help sectors coordinate with multiple States that rely on a common set of CI/KR. In many instances, State homeland security advisors 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 individual SCCs or GCCs or cross-sector councils. Additionally, DHS may selectively convene regionally based councils to address issues that cross sectors or jurisdictions, as required.

4.1.4 International CI/KR Protection Cooperation

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

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

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

4.1.4.1 Cooperation With International Security Partners

DHS, in coordination with the Department of State, works with international partners and other entities involved in the international aspects of CI/KR protection to exchange experiences, share information, and develop a cooperative environment to materially improve U.S. CI/KR protection. DHS, the Department of State, 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 CI/KR protection.

While SSAs and owners and operators are responsible for developing CI/KR 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 CI/KR protection:

- **International Outreach Program:** DHS, in cooperation with the Department of State and other Federal agencies, carries out international outreach activities to engage foreign governments and international/multinational organizations to promote a global culture of physical and cyber security. These outreach activities enable international cooperation and engage constituencies that often do not traditionally address CI/KR protection. This outreach encourages the development and adoption of best practices, training, and other programs designed to improve the protection of U.S. CI/KR overseas, as well as the reliability of international CI/KR on which this country depends. Other Federal, State, local, tribal, and private sector entities also engage in international outreach that may be related to CI/KR risk mitigation in situations where they work directly with their foreign counterparts.
- **The National Exercise Program:** DHS provides overarching coordination for the National Exercise Program to ensure the Nation's readiness to respond in an all-hazards environment and to practice and evaluate the steady-state protection plans and programs put in place by the NIPP. This exercise program engages international partners to address cooperation and cross-border issues, including those related to CI/KR protection. DHS and other security partners also participate in exercises sponsored by international partners.
- **National Cyber Exercises:** DHS and its security partners conduct exercises to identify, test, and improve coordination of the cyber incident response community, including Federal, State, regional, local, tribal, and international government elements, as well as private sector corporations and coordinating councils.

4.1.4.2 Implementing Current Agreements

Existing agreements with international security partners include bilateral and multilateral partnerships that have been entered into with the assistance of the Department of State. The key partners involved in existing agreements include:

- **Canada and Mexico:** CI/KR 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 infrastructures 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 CI/KR 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:** DHS has 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.
- **Group of Eight:** The G8 underscored its determination to combat all forms of terrorism and to strengthen international cooperation when heads of government attending the July 2005 meeting in Scotland issued a Statement on Counter-Terrorism, citing three areas of focus related to CI/KR protection:
 - To improve the sharing of information on the movement of terrorists across international borders;
 - To assess and address the threat to the transportation infrastructure; and
 - To promote best practices for rail and metro security.
- **North Atlantic Treaty Organization:** NATO addresses CI/KR 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 CI/KR 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.

4.1.4.3 Approach to International Cyber Security

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 to

address cyber security internationally. For example, the U.S.-based Information Technology Association of America participates in international cyber security 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 across the globe:

- **International Cyber Security Outreach:** DHS, in cooperation with the Department of State, 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 cyber security 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 cyber security and critical information infrastructure protection. For example, the Asia-Pacific Economic Cooperation 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, 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) G8 High-Tech Crime Working Group's principles for fighting cyber crime and protecting critical information infrastructure, (2) OECD guidelines on information and network security, and (3) 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 cyber security policy and operational cooperation. Leveraging pre-existing relationships among Computer Security Incident Response Teams (CSIRTs), DHS has

established a preliminary framework for cooperation on cyber security policy, watch and warning, and incident response with Australia, Canada, New Zealand, and the United Kingdom. The framework also incorporates efforts on strategic issues as agreed upon by these allies. DHS is also participating in the establishment of an International Watch and Warning Network (IWWN) among cyber security policy, computer emergency response, and law enforcement participants from 15 countries. The IWWN will provide a mechanism for the participating countries to share information to build global cyber situational awareness and coordinate incident response.

- **Partnerships to Address Cyber Aspects of CI/KR 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 cyber security as part of CI/KR 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 bi-national basis. In the context of the JCG, DHS established an action plan to address cyber security, watch, warning, and incident response, and other strategic initiatives.

4.1.4.4 Foreign Investment in CI/KR

CI/KR 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 impacts of proposed foreign investments on CI/KR protection, government monitoring activities aimed at ensuring compliance with agreements that result from CFIUS rulings, and supporting executive branch reviews of telecommunications applications to the FCC from foreign entities to assess if they pose any national security threat to CI/KR (see appendix 1B.4.4).

4.2 Information Sharing: A Network Approach

The effective implementation of the NIPP is predicated on active participation by government and private sector security partners in robust multi-directional information sharing. When owners and operators are provided with a comprehensive picture of threats or hazards to CI/KR and participate in ongoing multi-directional information flow, their ability to assess risks, make prudent security investments, and take protective actions is substantially enhanced. Similarly, when the government is equipped 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 multi-directional 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 communications, coordination, and information-sharing capabilities for all security partners;
- Provide security partners with a robust communications framework tailored to their specific information-sharing requirements, risk landscape, and protective architecture;
- Provide security 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 security partners with timely incident reporting and verification of related facts that CI/KR owners and operators can use with confidence when considering how evolving incidents might affect their security posture;
- Provide a means for State, local, tribal, and private sector security partners to be integrated, as appropriate, into the intelligence cycle, to include providing inputs to the intelligence requirements development process;
- Enable the flow of information required for security partners to assess risks, conduct risk management activities, invest in security measures, and allocate resources; and
- Protect the integrity and confidentiality of sensitive information.

The information-sharing process is designed to communicate both actionable information on threats and incidents and information pertaining to overall CI/KR status (e.g., plausible threats, vulnerabilities, potential consequences, incident situation, and recovery progress) so that owners and operators, States, localities, tribal governments, and other security partners can assess risks, make appropriate security investments, and take effective and efficient protective actions.

4.2.1 Information Sharing Between NIPP Security Partners

The primary objective of the NIPP network approach to information sharing is to enhance situational awareness and maximize the ability of government and private sector security partners at all levels to assess risks and execute risk-mitigation programs and activities. Implementation of the Nation's CI/KR protection mission depends on the ability of the government to receive and provide timely, actionable information on emerging threats to CI/KR owners and operators and security professionals so that they can take the necessary steps to mitigate risk.

Ongoing and future initiatives generally fall within one of three overarching categories:

- **Planning:** All security partners have a stake in setting the individual information requirements that best suit the needs of each CI/KR sector. DHS, in conjunction with SSAs and other State, local, tribal, and private sector security partners, will collaboratively develop and disseminate an Annual CI/KR Protection Information Requirements Report that summarizes the sectors' input and makes recommendations for collecting information requirements. The Information Requirements Report will be disseminated to the sectors through the SCCs. In addition to this process, DHS will coordinate with the Intelligence Community to support information collection that reflects the emerging requirements provided by SSAs and State, local, tribal, and private sector partners.
- **Information Collection:** Private sector participation in information collection is voluntary 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 with government-collected information to produce comprehensive threat assessments and threat warning products. DHS assessments, excluding PCII information, are shared across the sectors through electronic dissemination, posting to Homeland Security Information Network (HSIN) portals, and direct outreach by DHS/OIP sector specialists and DHS/HITRAC analysts. These efforts provide the private sector with timely, actionable information to enhance situational awareness and enable security planning activities.

- **Analysis and Decisionmaking:** DHS/HITRAC is responsible for integrating CI/KR specific vulnerability and consequence data with threat information to produce actionable risk assessments used to inform CI/KR risk-mitigation activities at all levels. DHS/HITRAC analysts work closely with CI/KR sector subject matter experts to ensure that these products address the individual requirements of each sector and help actuate corresponding security activities.

4.2.2 Information-Sharing Life Cycle

Planning, information collection, analyses, and decisionmaking are key elements of the CI/KR information life cycle. Protection of sensitive information and dissemination of actionable information are central tenets that are maintained throughout each stage of the life cycle.

4.2.2.1 Information Requirement

The information-sharing process begins with defining the information collection requirements to be adopted by field entities, analytic entities, and all other security partners that collect and disseminate intelligence and other security-related information.

4.2.2.2 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 that 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 security partners to maintain appropriate and protected information-sharing practices.

4.2.2.3 Top-Down and Bottom-Up Sharing

During incident situations, DHS monitors risk management activities and CI/KR status at the functional/operations level, the local law enforcement level, and at the cross-sector level. Information sharing may also incorporate information that comes from pre- and post-event natural disaster warnings and reports.

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 subsequently is routed to State and local governments, CI/KR 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 CI/KR-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 security 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.

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, as appropriate, to support further analysis or action as required. In the context of evolving threat or incident situations, 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 specific analysis and needs of these operations personnel.

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, restoration 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 security partners according to appropriate information protection protocols.

4.2.2.4 Decisions and Actions

Information sharing, whether top-down or bottom-up, is a means to an end. The objective of the information-sharing life cycle is to provide timely and relevant information that

Figure 4-2: NIPP Networked Information-Sharing Approach



security partners can use to make decisions and take necessary actions to manage CI/KR risk.

4.2.3 The Information-Sharing Approach

Figure 4.2 illustrates the broad concept of the NIPP multi-directional networked information-sharing approach. This information-sharing network consists of components that are connected by a national Web-based communications platform, known as the HSIN, so that security partners can obtain, analyze, and share information. The diagram illustrates how the HSIN is used for two-way and multi-directional information sharing between 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). Security partners

are grouped into nodes in the information-sharing network approach.

4.2.3.1 Information Sharing With HSIN

When fully deployed, the HSIN will constitute a robust and significant information-sharing system that supports NIPP-related steady-state CI/KR protection and NRP-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 the nodes 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, SSAs, and other security partners to share information. Other supporting technologies and more traditional methods of communications will continue to support CI/KR protection, as appropriate, and will be fully integrated into the network approach.

DHS and the SSAs work with other security partners to measure the efficacy of the network and to identify areas in which new mechanisms or supporting technologies are required. The HSIN and the key nodes of the NIPP information-sharing approach are detailed in the subsequent sections. By offering a user-friendly, efficient conduit for information sharing, HSIN enhances the combined effectiveness of all security partners 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 for all security partner command or watch centers, including those of supporting emergency management and public health activities.

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 information-sharing environment (ISE) for terrorism 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. HSIN will be one part of the ISE, and when fully developed, users of HSIN 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 security 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 information requirements, mission emphasis, or interest level. Within the Homeland Security Information Network for Critical Sectors (HSIN-CS) COI, each sector establishes rules for participation, including vetting and verification processes that are appropriate for the sector CI/KR landscape and requirements for information protection. For example, in some sectors, applicants are vetted through the SCC or ISAC; others may require participants to be documented members of a specific profession, such as law enforcement.

4.2.4 The Federal Intelligence Node

The Federal Intelligence Node, comprised of national Intelligence Community agencies, SSA intelligence offices, and the DHS Office of Intelligence and Analysis

(DHS/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 fusion center entities that contribute to information sharing in the context of the CI/KR protection mission.

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

- **DHS/HITRAC** analyzes and integrates threat information and works closely with components of the Federal Infrastructure Node to generate and disseminate threat warning products to security partners, both internal and external to the network, as appropriate.
- 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.

Project Seahawk is a task force comprised of 40 Federal, State, and local law enforcement agencies that enhances intermodal transportation and port security by sharing jurisdictional responsibility for the Port of Charleston and its metropolitan area. Other examples of information-sharing and intelligence fusion center entities include:

- **DHS/USCG** operates a Maritime Intelligence Fusion Center (MIFC)—Pacific (Alameda, CA) and an MIFC—Atlantic (Dam Neck, VA). These centers serve as resources for intelligence support for the DHS/USCG, as well as for local and international maritime, intelligence, and law enforcement partners;
- **DHS/Immigration and Customs Enforcement** operates the Human Smuggling and Trafficking Center, an inter-agency joint intelligence fusion center focused specifically on human smuggling and human trafficking. Other DHS entities, the Department of State, DOJ, and other members of the Intelligence Community participate in the Center; and
- The **Defense Intelligence Agency** operates intelligence analytic fusion centers in the various overseas areas of operation (i.e., EUCOM, PACOM, CENTCOM, SOUTHCOM, NORTHCOM). These fusion cells support production coordination and targeting/operational activities, as well as ongoing area operations or special programs.

- The **NCTC** serves as the primary Federal organization for analyzing and integrating all intelligence possessed or acquired by the U.S. Government pertaining to terrorism and counterterrorism, except purely domestic counterterrorism information. The NCTC may, 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 **National Maritime Intelligence Center** serves as the central point of connectivity to fuse, analyze, and disseminate information and intelligence for shared situational awareness across classification boundaries.

At the regional and field levels, Federal information-sharing and intelligence fusion 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.

4.2.5 The Federal Infrastructure Node

The Federal Infrastructure Node, comprised of DHS, SSAs, 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 CI/KR and facilitates the development and dissemination of appropriate real-time threat and warning products and corresponding protective measures recommendations to security partners (see chapter 3). Participants in the Federal node collaborate with CI/KR owners and operators to gain input during the development of threat and warning products and corresponding protective measures recommendations.

4.2.6 State, Local, Tribal, and Regional Node

This node provides links between DHS, the SSAs, and security partners at the State, local, regional, and tribal 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 security partners. The NIPP network approach augments these established communications channels by facilitating two-way and multi-directional information sharing between various security partners. Members of this node provide incident response, first-responder information, and reports of suspicious activity to the FBI and DHS for 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 between 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 CI/KR protection.

Additionally, DHS protective security advisors (PSAs) serve as liaisons to CI/KR owners and operators, as well as State, local, and tribal officials. PSAs assist efforts to identify, assess, monitor, and minimize risk to CI/KR at the regional, State, or local level. PSAs facilitate, coordinate, and/or perform vulnerability assessments in support of local CI/KR owners and operators, and assist with security efforts coordinated through State homeland security advisors, as requested by State, local, or tribal authorities.

4.2.7 Private Sector Node

The Private Sector Node includes CI/KR 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 CI/KR owners and operators.

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

ISACs provide an example of an effective private sector information-sharing and analysis mechanism. Originally recommended by Presidential Decision Directive 63 (PDD-63) in 1998, ISACs are sector-specific entities that advance physical and cyber CI/KR protection efforts by establishing and maintaining frameworks for operational interaction between and among members and external security partners. ISACs 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 appropriate governmental agencies; identifying and disseminating knowledge and best practices; and promoting education and awareness.

The sector partnership model recognizes that not all CI/KR sectors have established ISACs. Each sector has the ability to implement a tailored information-sharing solution that may include ISACs; 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. Most ISACs are members of the ISAC Council, which provides the mechanism for the inter-sector sharing of operational information. Sectors that do not have ISACs per se use other mechanisms that participate in the HSIN and other CI/KR protection information-sharing arrangements. For the purposes of the NIPP, these operationally oriented groups are also referred to collectively as ISACs.

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

4.2.8 DHS Operations Node

The DHS Operations Node maintains close working relationships with other government and private sector security partners to enable and coordinate an integrated operational picture, provide operational and situational awareness, and facilitate CI/KR information sharing within and across sectors. DHS and other Federal watch/operations centers provide the 24/7 capability required to enable the real-time alerts and warnings, incident reporting, situational awareness, and assessments needed to support CI/KR 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 upon 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 with security partners, providing a far-reaching network of awareness and coordination.

4.2.8.1 National Operations Center²¹

The NOC, formerly known as the Homeland Security Operations Center, serves as the Nation's hub for domestic incident management operational coordination and situational awareness. The NOC is a standing 24/7 interagency organization 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 among security partners. 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 security 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 partners in the FBI, Intelligence Community, and other Federal departments and agencies on a continuous basis. When a threat is determined to be credible and 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.

²¹ *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.

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 e-mail 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 level of the HSAS.
- **Homeland Security Assessments:** Communicate threat information that does not meet the timeliness, specificity, or criticality criteria of an advisory, but is pertinent to the security of U.S. CI/KR.

The NOC is comprised of 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 center that provides overall coordination of Federal response, recovery, and mitigation activities, and emergency management program implementation.
- **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 is a 24/7 watch/operations center that maintains ongoing operational and situational awareness of the Nation's CI/KR sectors. As a CI/KR-focused element of the NOC, the NICC provides a centralized mechanism and process for information sharing and coordination between the

government, SCCs, GCCs, and other industry partners. The NICC receives situational, operational, and incident information from the CI/KR sectors, in accordance with information-sharing protocols established in the NRP. The NICC also disseminates products originated by HITRAC that contain all-hazards warning, threat, and CI/KR 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 CI/KR. 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.
- **National Response Planning and Execution:** The NICC supports the NRP by facilitating information sharing among SCCs, GCCs, ISACs, and other security partners during CI/KR mitigation, response, and recovery activities.

4.2.8.2 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 NCC, which is a joint industry-government entity. Under the Executive order, the NCC assists the NCS in the initiation, coordination, restoration, and reconstitution of national security or emergency preparedness 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.

4.2.8.3 United States Computer Emergency Readiness Team

The United States Computer Emergency Readiness Team (US-CERT) is a 24/7 single point of contact for cyberspace analysis, warning, information sharing, and incident response and recovery for security 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 security partners to disseminate reasoned and actionable cyber security information through a Web site, accessible via the HSIN, and through mailing lists. Among the products it provides are:

- **Cyber Security Bulletins:** Weekly bulletins written for systems administrators and other technical users that summarize published information concerning new security issues and vulnerabilities.
- **Technical Cyber Security Alerts:** Written for system administrators and experienced users, technical alerts provide timely information on current security issues, vulnerabilities, and exploits.
- **Cyber Security 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.
- **Cyber Security 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 cyber security 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 cyber security. The private sector can use the protections afforded by the Critical Infrastructure Information Act to electronically submit proprietary data to US-CERT.

4.2.9 Other Information-Sharing Nodes

DHS, other Federal agencies, and the law enforcement community provide additional services and programs that share information supporting CI/KR protection with a broad range of security 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 e-mail, 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 between the FBI, other government 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. CI/KR from physical and cyber threats.
- **Interagency Cyber Security Efforts:** The intelligence and law enforcement communities have various information-sharing mechanisms in place. Examples include:
 - **U.S. Secret Service's Electronic Crimes Task Forces:** U.S. Secret Service's Electronic Crimes Task Forces (ECTFs) prevent, detect, and investigate electronic crimes, cyber-based attacks, and intrusions against CI/KR 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.
- **CEO COM LINKSM:** The Critical Emergency Operations Communications Link (CEO COM LINK) is a telephone communications system that will enable the Nation’s top chief executive officers (CEOs) to enhance the protection of employees, communities, and the Nation’s CI/KR by communicating with government officials and each other about specific threats or during national crises. The calls, which are restricted to authorized participants, allow top government officials to brief CEOs on developments and threats, and allow CEOs to ask questions or share information with government leaders and with each other.

4.3 Protection of Sensitive CI/KR Information

NIPP implementation will rely greatly on critical infrastructure information provided by the private sector. 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 CI/KR 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 CI/KR information is properly safeguarded. In addition to PCII, other programs and procedures used to protect sensitive information include Sensitive Security Information for transportation activities, Unclassified Controlled Nuclear Information (UCNI), 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 Act of 2002. The program provides a means for sharing private sector information with the government while providing assurances that the information will be exempt from public disclosure and will be properly safeguarded. This enables members of the private sector to voluntarily submit sensitive information regarding CI/KR to DHS with the assurance that the information will be protected.

The PCII Program, which operates under the authority of the Critical Infrastructure Information (CII) Act and interim implementing regulations (6 Code of Federal Regulations (CFR) Part 29 (the Interim Rule)), defines the requirements for submitting CII and the requirements that government 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, and is presently working on rulemaking that will replace the interim regulations and make the program even stronger. 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 government and the private sector, and assuring that programs receiving voluntary submissions of PCII use proper procedures to continuously safeguard that information. The Program Office works with government organizations and the private sector to develop information-sharing partnerships that promote greater homeland security through validated protection programs and procedures.

4.3.1.2 Critical Infrastructure Information Protection

The following process and procedures apply to all CII submissions:

- Individuals or collaborative groups may submit information for protection;
- The PCII Program Office validates that the information qualifies for protection under the act;

- All validated PCII is stored in a secure data management system and security partners follow DHS sharing guidelines for unclassified but sensitive information;
- Secure methods are used for disseminating PCII;
- Authorized users must comply with safeguarding requirements defined by the PCII Program Office; and
- Any suspected disclosure of PCII will be promptly investigated.

4.3.1.3 Uses of PCII

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

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

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

- In furtherance of an investigation or the prosecution of a criminal act;
- To either House of Congress, or to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee thereof or subcommittee, or any such joint committee; or
- To the Comptroller General or any authorized representative of the Comptroller General, in the course of the performance of the duties of the General Accounting Office.

4.3.1.4 PCII Protections and Authorized Users

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

- Used appropriately for homeland security purposes;

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

The law and rule prescribe criminal penalties for intentional unauthorized access, distribution, and misuse of PCII 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 sanctions provided for under the CII Act for unauthorized disclosure of PCII apply only to Federal personnel. State and local participating entities may have their own penalties for improperly handling sensitive information and these entities may lose future access to PCII.

4.3.2 Other Information Protection Protocols

Information protection protocols may impose requirements for access or other standard processes for safeguarding information. Information need not be designated as CII to receive security protection and disclosure restrictions. Several categories of information related to CI/KR are considered to be sensitive but unclassified and require protection. Examples include sector-specific information, such as sensitive transportation or nuclear information, or information determined to be classified information based on the analysis of unclassified information. The major categories that apply to CI/KR are discussed below.

4.3.2.1 Sensitive Security Information

The Maritime Transportation Security Act, the Aviation Transportation Security Act, and the Homeland Security Act establish protection for Sensitive Security Information (SSI). 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 sector owners and operators.

4.3.2.2 Unclassified Controlled Nuclear Information

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 Freedom of Information Act Exemptions and Exclusions

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

4.3.2.4 Classified Information

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

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

- The information can only be designated as classified by a duly empowered authority;
- The information must be owned by, produced by or for, or under the control of the Federal Government;
- The unauthorized disclosure of the information reasonably could be expected to result in identifiable damage to U.S. national security; and
- Only information related to the following may be classified:
 - Military plans, weapons systems, or operations;
 - Foreign government information;
 - Intelligence activities (including special activities), intelligence sources or methods, or cryptology;
 - Foreign relations or foreign activities of the United States, including confidential sources;
 - Scientific, technological, or economic matters 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 CI/KR protection have these characteristics. This information may be determined to be classified information and protected accordingly.

4.3.2.5 Physical and Cyber Security Measures

DHS uses strict information security protocols for the access, use, and storage of sensitive information, including that related to CI/KR. These protocols include both physical security measures and cyber security 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 NADB.

4.4 Privacy and Constitutional Freedoms

Mechanisms detailed in the NIPP are designed to provide a balance between achieving a high level of security and protecting the civil rights and liberties that form an integral part of America's national character. Achieving this balance requires acceptance of some level of risk. In providing for effective protective 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 personal information. The following DHS offices support the NIPP processes:

- **DHS Privacy Office:** Pursuant to the Homeland Security Act, DHS has designated a privacy officer to ensure that it appropriately balances the mission with civil liberty and privacy concerns. The officer consults regularly with privacy advocates, industry experts, and the public at large to 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, DHS has established an Office for Civil Rights and Civil Liberties to review and assess allegations of abuse of civil rights or civil liberties, racial or ethnic profiling, and to provide advice to DHS components.

