

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

This chapter describes the linkages between the NIPP, the SSPs, and other CI/KR protection strategies, plans, and initiatives that are most relevant to the overarching national homeland security and CI/KR protection missions. It also describes how the unified national CI/KR protection effort integrates with the prevention, protection, response, and recovery elements of the homeland security mission. Sector-specific linkages to these other national frameworks are more appropriately addressed in the SSPs.

5.1 A Coordinated National Approach to the Homeland Security Mission

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

5.1.1 Legislation

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

other statutes (as described in chapter 2 and appendix 2A) provide authorities for cross-sector and sector-specific CI/KR protection activities. SSPs will address relevant sector-specific authorities.

5.1.2 Strategies

The National Strategy for Homeland Security, the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, and the National Strategy to Secure Cyberspace together provide the vision and strategic direction for the CI/KR protection elements of the homeland security mission (see figure 5-1, columns 1 and 2). A number of other Presidential strategies, such as the National Intelligence Strategy, provide direction and guidance related to CI/KR protection on a national or sector-specific basis (see appendix 2A).

5.1.2.1 The National Strategy for Homeland Security

The President's National Strategy for Homeland Security established protection of America's CI/KR as a core homeland security mission and as a key element of the comprehensive approach to homeland security and domestic incident

management. This strategy articulated the vision for a unified “American Infrastructure Protection effort” to “ensure we address vulnerabilities that involve more than one infrastructure sector or require action by more than one agency,” and to “assess threats and vulnerabilities comprehensively across all infrastructure sectors to ensure we reduce the overall risk to the country, instead of inadvertently shifting risk from one potential set of targets to another.”

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

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

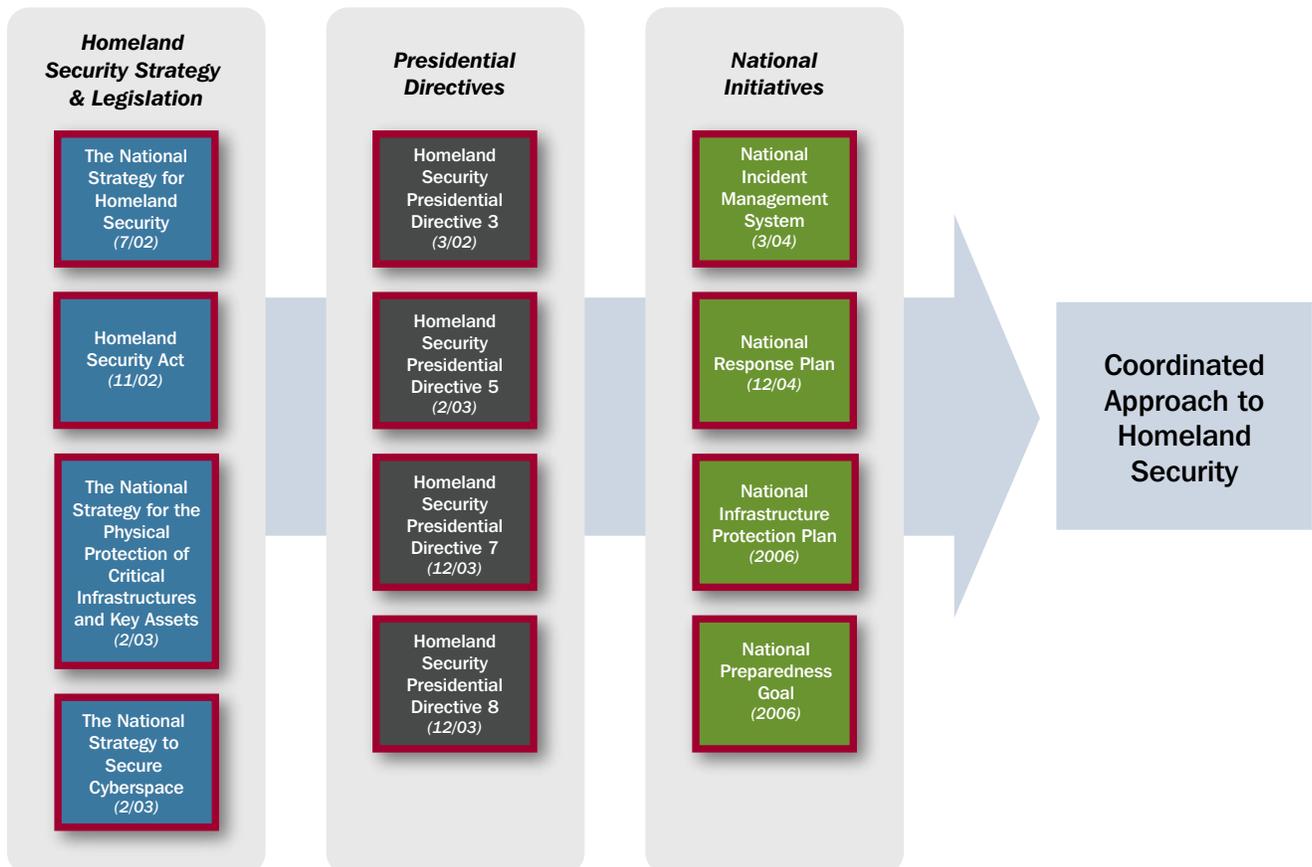
The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets identifies national policy, goals, objectives, and principles needed to “secure the

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

5.1.2.3 The National Strategy to Secure Cyberspace

The National Strategy to Secure Cyberspace sets forth objectives and specific actions needed to prevent cyber attacks against America’s CI/KR; identifies and appropriately responds to those responsible for cyber attacks; reduces nationally identified vulnerabilities; and minimizes damage and recovery time from cyber attacks. This strategy articulates five national priorities, including the establishment of a security response system, a threat and vulnerability reduction

Figure 5-1: National Framework for Homeland Security



program, awareness and training programs, efforts to secure government cyberspace, and international cooperation.

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

5.1.3 Homeland Security Presidential Directives and National Initiatives

Homeland Security Presidential directives set national policies and executive mandates for specific programs and activities (see figure 5-1, column 3). The first was issued on October 29, 2001, shortly after the attacks on September 11, 2001, establishing the Homeland Security Council. It was followed by a series of directives regarding the full spectrum of actions required to “prevent terrorist attacks within the United States; reduce America’s vulnerability to terrorism, major disasters, and other emergencies; and minimize the damage and recover from incidents that do occur.” A number of these are relevant to CI/KR protection. HSPD-3, Homeland Security Advisory System, provides the requirement for the dissemination of information regarding terrorist acts to Federal, State, and local authorities, and the American people. HSPD-5 addresses the national approach to domestic incident management; HSPD-7 focuses on the CI/KR protection mission; and HSPD-8 focuses on ensuring the optimal level of preparedness to protect, prevent, respond to, and recover from terrorist attacks and the full range of natural and manmade hazards.

This section addresses the Homeland Security Presidential directives that are most relevant to the overarching CI/KR protection component of the homeland security mission (e.g., HSPDs 3, 5, 7, and 8). Other Presidential directives, such as HSPD-9, Defense of the United States Agriculture and Food, and HSPD-10, Biodefense for the 21st Century, are relevant to CI/KR protection in specific sectors and will be addressed in further detail in the appropriate SSPs.

5.1.3.1 HSPD-3, Homeland Security Advisory System

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

alert. The threat conditions also serve as guideposts for the implementation of tailored protective measures by State, local, tribal, and private sector security partners.

5.1.3.2 HSPD-5, Management of Domestic Incidents

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

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

The NRP (December 2004) was built on the NIMS template, signed by 29 Federal departments and agencies and 3 nongovernmental organizations, and fully implemented on April 14, 2005. It establishes a single, comprehensive framework for the management of domestic incidents (including threats) that require DHS coordination and effective response by an appropriate combination of Federal, State, local, and tribal governments; the private sector; and nongovernmental organizations.

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

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

- A strategy to identify and coordinate the protection of CI/KR;
- A summary of activities to be undertaken to prioritize, reduce the vulnerability of, and coordinate protection of CI/KR;
- A summary of initiatives for sharing information and for providing threat and warning data to State, local, and tribal governments and the private sector; and

- Coordination and integration, as appropriate, with other Federal emergency management and preparedness activities, including the NRP and guidance provided in the National Preparedness Goal.

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

5.1.3.4 HSPD-8, National Preparedness

HSPD-8 (December 2003) mandates development of a National Preparedness Goal (see figure 5-1, column 4) aimed at helping entities at all levels of government build and maintain the capabilities to prevent, protect against, respond to, and recover from major events “to minimize the impact on lives, property, and the economy.”

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

The National Preparedness Goal uses capabilities-based planning processes and enables Federal, State, local, and tribal entities to prioritize needs, update strategies, allocate resources, and deliver programs. The goal references standard planning tools that are applicable to implementation of the NIPP, including the UTL and the TCL. The UTL provides a menu of tasks from all sources that may be performed

to implement CI/KR protection programs, as well as those needed to respond to major incidents. The TCL provides guidance on the specific capabilities and levels of capability relevant to CI/KR protection and other areas of the homeland security mission that Federal, State, local, and tribal entities will be expected to develop and maintain. These will vary based on the risk and the needs of the various entities involved. Like the NIPP, the UTL and TCL are living documents that will be enhanced and refined over time.

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

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

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

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

The NIPP risk management framework, sector partnership model, and information-sharing mechanisms are structured to support coordination and cooperation with private sector owners and operators while recognizing the differences between and within sectors, acknowledging the need to protect sensitive information, establishing processes for

information sharing, and providing for smooth transitions from steady-state operations to incident response.

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

The NIPP Base Plan, Appendixes, and SSPs outline the overarching elements of the CI/KR protection effort that generally are applicable within and across all sectors. The SSPs are an integral component of the NIPP and exist as independent documents to address the unique perspective, risk landscape, and methodologies associated with each sector. Homeland security plans and strategies at the State, local, and tribal levels of government address CI/KR protection within their respective jurisdictions, as well as mechanisms for coordination with various regional efforts and other external entities. The NIPP also is designed to work with the range of CI/KR protection-related plans and programs instituted by the private sector, both through voluntary actions and as a result of various regulatory requirements. These plans and programs include business continuity and resilience measures. NIPP processes are designed to enhance coordination, cooperation, and collaboration among security partners within and across sectors to synchronize related efforts and avoid duplicative or unnecessarily costly security requirements.

5.3.1 Sector-Specific Plans

Based on guidance from DHS, SSPs are developed jointly by SSAs in close collaboration with SCCs, GCCs, and others, including State, local, and tribal homeland security partners with key interests or expertise appropriate to the sector. The SSPs provide the means by which the NIPP is implemented across all sectors, as well as a national framework for each sector that guides the development, implementation, and updating of State and local homeland security strategies and CI/KR protection programs. Generally, SSPs will be unclassified; some SSPs or portions of SSPs containing sensitive information may be classified and subject to more stringent document control and limited distribution to security partners with appropriate clearances and a need to know.

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

- Define sector security partners, authorities, regulatory bases, roles and responsibilities, and interdependencies;

- Establish or institutionalize already existing procedures for sector interaction, information sharing, coordination, and partnership;
- Establish the goals and objectives, developed collaboratively between security partners, required to achieve the desired protective posture for the sector;
- Identify international considerations;
- Identify areas for government action above and beyond an owner/operator or sector risk model; and
- Identify the sector-specific approach or methodology that SSAs, in coordination with DHS and other security partners, will use to conduct the following activities consistent with the NIPP framework:
 - Identify priority CI/KR and functions within the sector, including cyber considerations;
 - Assess sector risks, including potential consequences, vulnerabilities, and threats;
 - Assess and prioritize assets, systems, networks, and functions of national-level significance within the sector;
 - Develop risk-mitigation programs based on detailed knowledge of sector operations and risk landscape;
 - Provide protocols to transition between steady-state CI/KR protection and incident response in an all-hazards environment;
 - Use metrics to measure and communicate program effectiveness and risk management within the sector;

Figure 5-2: Sector-Specific Plan Structure



- Address R&D requirements and activities relevant to the sector; and
- Identify the process used to promote governance and information sharing within the sector.

The structure for the SSPs is shown in figure 5-2; it facilitates cross-sector comparisons and coordination by DHS and other SSAs.

The SSPs must be completed and submitted by the SSAs to DHS within 180 days of issuance of the NIPP. The SSP concurrence process includes a formal review process for GCC member departments and agencies, as well as demonstrated/documentated collaboration and coordination with the SCC, which may include letters of endorsement or statements of concurrence.

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

The National Preparedness Goal defines the development and implementation of a CI/KR protection program as a key component of State, regional, local, and tribal homeland security programs. Creating and managing a CI/KR protection program for a given jurisdiction entails building an organizational structure and mechanisms for coordination between government and private sector entities that can be used to implement the NIPP risk management framework. This includes taking actions within the jurisdiction to set security goals; identifying assets, systems, and networks; assessing risks; prioritizing CI/KR across sectors and jurisdictional levels; implementing protective programs; measuring the effectiveness of risk management efforts; and sharing information between relevant public and private sector security partners. These elements form the basis of focused CI/KR protection programs and guide the implementation of the relevant CI/KR protection-related goals and objectives outlined in State, local, and tribal homeland security strategies.

In a regional context, the NIPP risk management framework and information-sharing processes can be applied through the development of a regional partnership model or the use of existing regional coordinating structures. Effective regional approaches to CI/KR protection involve coordinated information sharing, planning, and sharing of costs and risk. Regional approaches also include exercises to bring public and private sector partners together around a shared understanding of the challenges to regional resilience; analytical tools to inform decisionmakers on risk and risk management with the associated benefits and costs; and forums to enable

decisionmakers to formulate protective measures and identify funding requirements and resources within and across sectors and jurisdictions.

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

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

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

Private sector owners and operators develop and maintain plans for business risk management that include steady-state security and facility protection, as well as business continuity and emergency management plans. Many of these plans include heightened security requirements for CI/KR protection that address the terrorist threat environment. Coordination with these planning efforts is relevant to effective implementation of the NIPP. Private sector security partners are encouraged to consider the NIPP when revising these plans, and to work with government security partners to integrate their efforts with Federal, State, local, and tribal CI/KR protection efforts as appropriate.

5.4 CI/KR Protection and Incident Management

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

5.4.1 The National Response Plan

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

The NRP Base Plan and annexes provide protocols for coordination among various Federal departments and agencies; State, local, and tribal governments; and private sector partners, both for pre-incident prevention and preparedness, and post-incident response, recovery, and mitigation. The NRP specifies incident management roles and responsibilities, including emergency support functions designed to expedite the flow of resources and program support to the incident area. SSAs and other Federal departments and agencies have roles within the NRP structure that are distinct from, yet complementary to, their responsibilities under the NIPP. Ongoing implementation of the NIPP risk management framework, partnerships, and information-sharing networks sets the stage for CI/KR security and restoration activities within the NRP framework by providing mechanisms to quickly assess the impacts of the incident on both local and national CI/KR, assist in establishing priorities for CI/KR restoration, and augment incident-related information sharing with security partners.

5.4.2 Transitioning From NIPP Steady-State to Incident Management

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

DHS and security partners develop and implement stepped-up, protective actions to match the increased terrorist threat conditions specified by the HSAS, and to address various other all-hazards alerts and warning requirements. As warnings or threat levels increase, NRP coordinating structures are activated to enable incident management. DHS and security partners carry out their NRP responsibilities and also use the NIPP risk management framework to provide the CI/KR protection dimension needed to inform NRP incident command and control, and multi-agency coordination. When an incident occurs, regardless of the cause, the NRP is implemented for overall coordination of domestic incident management activities. The NIPP provides the CI/KR dimension, reinforcing NRP incident management coordinating structures and processes. Implementation of the NIPP risk management framework facilitates those actions directly related to the current threat status, as well as incident prevention, response, restoration, and recovery.

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

- Increasing protection levels to correlate with the specific threat vectors or threat level communicated through the HSAS or other relevant all-hazards alert and warning

systems, or in accordance with sector-specific warnings using the NIPP information-sharing networks;

- Using the NIPP information-sharing networks and risk management framework to review and establish national priorities for CI/KR protection; facilitating communications between security partners; and informing the NRP processes regarding priorities for response, recovery, and restoration of CI/KR within the incident area, as well as on a national scale;
- Fulfilling roles and responsibilities as defined in the NRP for incident management activities; and
- Working with sector-level information-sharing entities and owners and operators on information-sharing issues during the active response mode.