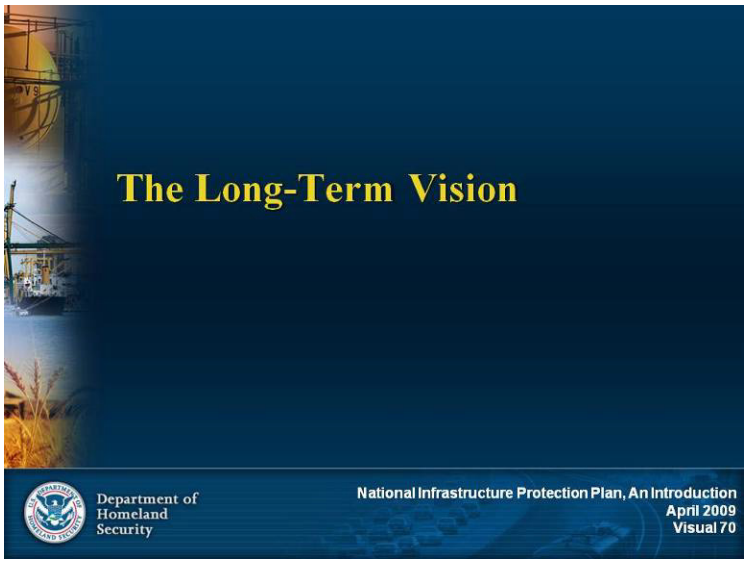
Topic | **The Long-Term Vision**

Visual 70



Visual Description: The Long-Term Vision

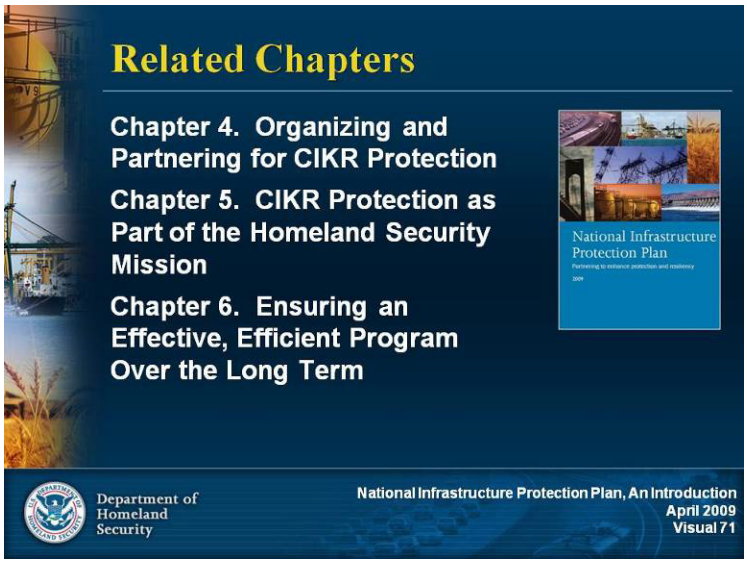
Instructor Notes

As you have learned, the NIPP defines the CIKR protection component of the homeland security mission. Implementing CIKR protection requires partnerships, coordination, and collaboration among all levels of government and the private sector. In this section, we'll look at how the NIPP:

- Fosters information sharing at all levels.
- Provides guidance on the structure and content of each Sector-Specific Plan, as well as the CIKR protection-related aspects of State and local homeland security plans.
- Helps to ensure an effective, efficient CIKR protection program over the long term.

Topic | **The Long-Term Vision**

Visual 71



Visual Description: Related Chapter

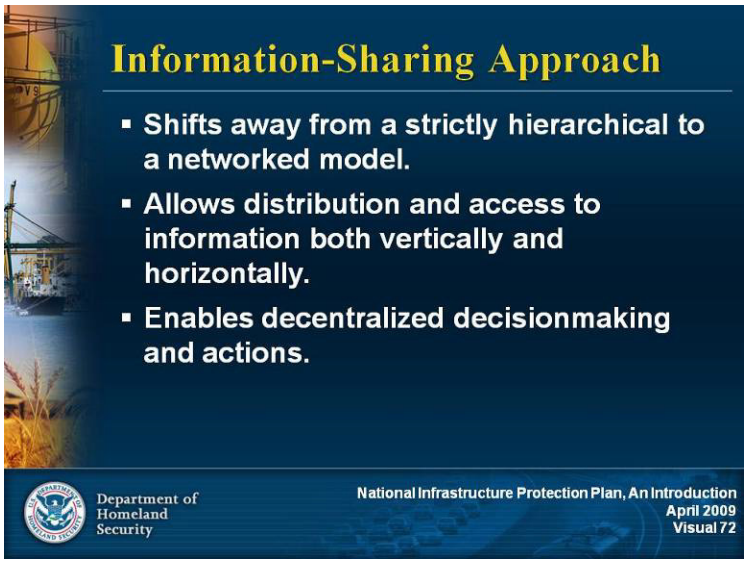
Instructor Notes

Additional information on the topics about to be presented can be found in in the following NIPP chapters:

- Chapter 4. Organizing and Partnering for CIKR Protection
- Chapter 5. CIKR Protection: As Part of the Homeland Security Mission
- Chapter 6. Ensuring an Effective, Efficient Program Over the Long Term.

Topic | **The Long-Term Vision**

Visual 72



Visual Description: Information-Sharing Benefits

Instructor Notes

Effective implementation of the NIPP is predicated on active participation by government and private sector partners in robust, multidirectional information sharing.

Information sharing enhances:

- Owners' and operators' ability to assess risks, make prudent security investments, and develop appropriate resiliency strategies.
- Government to adjust its information collection, analysis, synthesis, and dissemination activities based on the needs of the private sector.

The CIKR Information-Sharing Environment supports three levels of decisionmaking and action:

- Strategic planning and investment
- Situational awareness and preparedness
- Operational planning and response

Topic | **The Long-Term Vision**

Visual 73

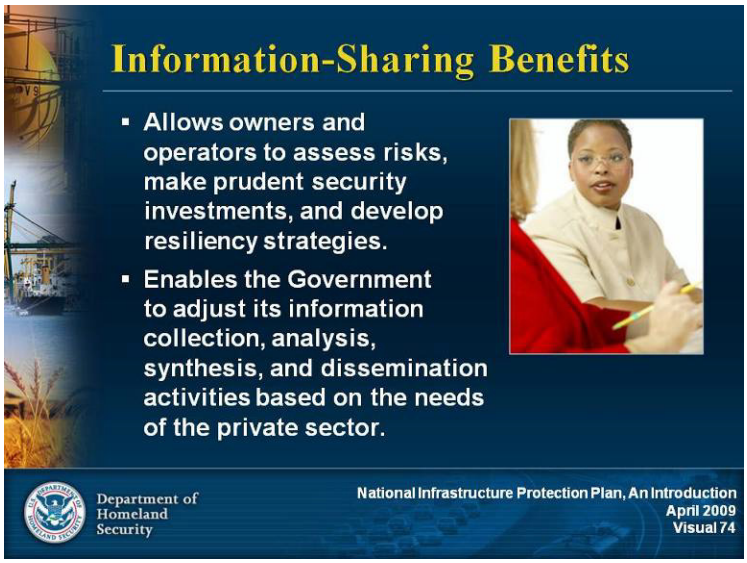
Visual Description: Information-Sharing Approach

Instructor Notes

The NIPP information-sharing approach uses a networked model, allowing distribution and access to information both vertically and horizontally, as well as the ability to enable decentralized decisionmaking and actions.

Topic | **The Long-Term Vision**

Visual 74



Visual Description: The NIPP Information-Sharing Approach: Networked Model

Instructor Notes

As illustrated in the visual, the NIPP information-sharing approach is 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 network consists of components that are connected by a national communications platform, the Homeland Security Information Network (HSIN). HSIN is one of the key DHS technology tools for strengthening the protection and ensuring the reliable performance of the Nation's CIKR through communication, coordination, and information sharing.

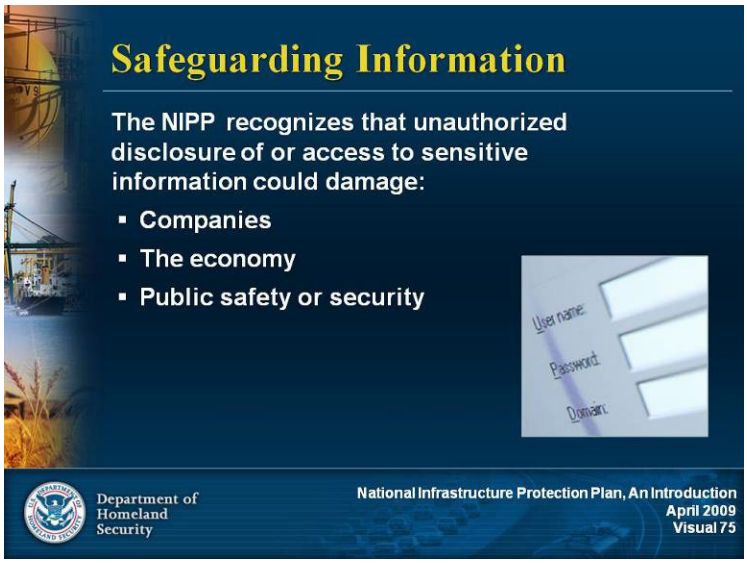
Note: A larger version of the illustration on the visual is provided on the following page.

Topic | **The Long-Term Vision**

Caption: Graphic showing an information-sharing model that depicts information flowing in all dimensions from DHS (fused information, situational and operational awareness coordination); the Federal Intelligence Community (credible threats and threat warning products); the Federal Infrastructure Community (CIKR status, CIKR risk environment, actions and programs); State, Territorial, local, tribal, and regional partners (incident response information, suspicious activities); and the private sector (incident information, suspicious activities, subject-matter expertise).

Topic The Long-Term Vision

Visual 75



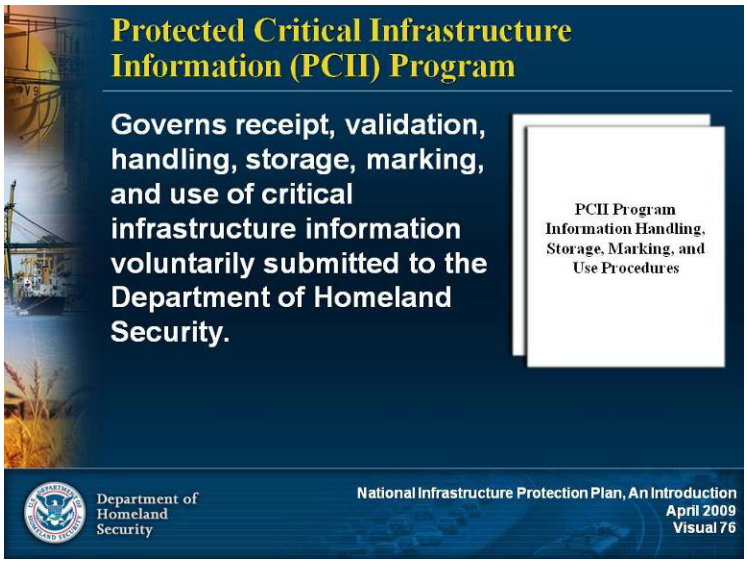
Visual Description: Safeguarding Information

Instructor Notes

NIPP implementation relies on the CIKR information provided by the private sector and State and local governments. The NIPP recognizes that the disclosure of sensitive business or security information could cause serious damage to companies, the economy, and public safety or security through unauthorized disclosure or access.

Topic | **The Long-Term Vision**

Visual 76



Visual Description: Protected Critical Infrastructure Information (PCII) Program

Instructor Notes

DHS and other Federal agencies use a number of programs and procedures, such as the Protected Critical Infrastructure Information (PCII) Program, to ensure that CIKR information is properly safeguarded.

The PCII Program includes procedures that govern the receipt, validation, handling, dissemination, storage, marking, and use of critical infrastructure information voluntarily submitted to the Department of Homeland Security. These procedures are also applicable to Federal, State, or local government employees or contractors supporting Federal agencies that have access to, handle, use, or store critical infrastructure information that enjoys protection under the Critical Infrastructure Information Act of 2002.

The PCII 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.
- Enables members of the private sector to voluntarily submit sensitive information regarding CIKR to DHS with the assurance that the information will be protected.
- Defines the requirements for submitting CII and the requirements that government entities must meet for accessing and safeguarding PCII.

Resource | **Fact Sheet—Protected Critical Infrastructure Information (PCII) Program Issuance Final Rule: Procedures for Handling Critical Infrastructure Information**

The Department of Homeland Security (DHS) issued the Final Rule on Procedures for Handling Critical Infrastructure Information on Friday, September 1, 2006. This rule finalizes the procedures for the Protected Critical Infrastructure Information (PCII) Program in governing the receipt, validation, handling, storage, marking, and use of critical infrastructure information voluntarily submitted to DHS.

What is the history of the Final Rule?

The Final Rule is the capstone to a series of legislative and regulatory actions that shaped the PCII Program. Congress passed the Critical Infrastructure Information (CII) Act of 2002 as part of the Homeland Security Act. A 90-day public comment period followed under the Notice of Proposed Rulemaking. The Interim Rule was issued in February 2004, when the PCII Program Office opened. The program operated under the Interim Rule while the Department completed the Final Rule.

What is the purpose of the PCII Program and what protections does it provide?

It is estimated that over 85 percent of the critical infrastructure upon which our national security, economy, and public welfare depend is owned and operated by the private sector. The PCII Program was created to encourage the private sector to voluntarily share security-related information about this infrastructure by providing special protection. Information submitted, if it satisfies the requirements of the CII Act, is protected from Freedom of Information Act disclosure, State and local disclosure laws, and use in civil litigation.

Additionally, PCII cannot be used as the basis for a regulatory action.

How does the Final Rule affect the PCII Program?

The Final Rule reinforces many of the safeguarding measures put in place by the Interim Rule and reflects a careful study of comments received from the public. The Final Rule makes the PCII Program more responsive to the submitters of critical infrastructure information and the users that rely upon it to secure the homeland.

Some of the key effects of the Final Rule are:

- Expansion of the definition of PCII, granting protection to information even if in the hands of the submitter.

  The Final Rule makes clear that critical infrastructure information submitted and validated for protection under the CII Act of 2002, the information and documents prepared, and drafts and copies retained by the submitter, and any discussions with DHS regarding the CII, shall be considered PCII and cannot be used directly in any civil litigation without the submitter's consent.

- Fewer circumstances under which PCII can lose its protected status, providing greater assurance for submitters. Whether CII provided to the PCII Program Manager is protectable will be determined at the time of submission. In response to submitters' concerns about the future status of their information, the Final Rule addresses criteria that required the removal of protected status.

- Categorical inclusion of classes of CII, allowing for presumptive validation and more certainty for submitters.

  The Final Rule invests the PCII Program Manager with the authority and flexibility to designate certain types of infrastructure information as presumptively valid PCII to accelerate the validation process. The PCII Program Manager may establish categories of information for which PCII status will automatically apply.

Resource | **Fact Sheet—Protected Critical Infrastructure Information (PCII) Program Issuance Final Rule: Procedures for Handling Critical Infrastructure Information**

- Submission of CII to other Federal agencies, providing for greater intake capability and greater convenience for submitters.

  The Final Rule identifies procedures for indirect submissions to DHS through DHS field representatives and other Federal agencies. Federal agencies other than DHS may be designated to receive CII on behalf of DHS, but only the PCII Program Manager is authorized to make the decision to validate a submission as PCII.

- State and local contractors permitted to receive PCII, providing for greater value and flexibility for our State and local partners.

  The Final Rule clarifies that State, local, and tribal contractors can receive PCII under the same conditions as Federal contractors. As in the case of Federal contractors, State, local, and tribal contractors are agents of the governmental entity, carrying out the functions on behalf of the government in furtherance of its mission and under its direction.

For more information about the PCII Program, please visit www.dhs.gov/pcii or contact the PCII Program Office by calling (202) 360-3023, or via email at pcii-info@dhs.gov.

Topic | **The Long-Term Vision**

Visual 77

Visual Description: Long-Term Success

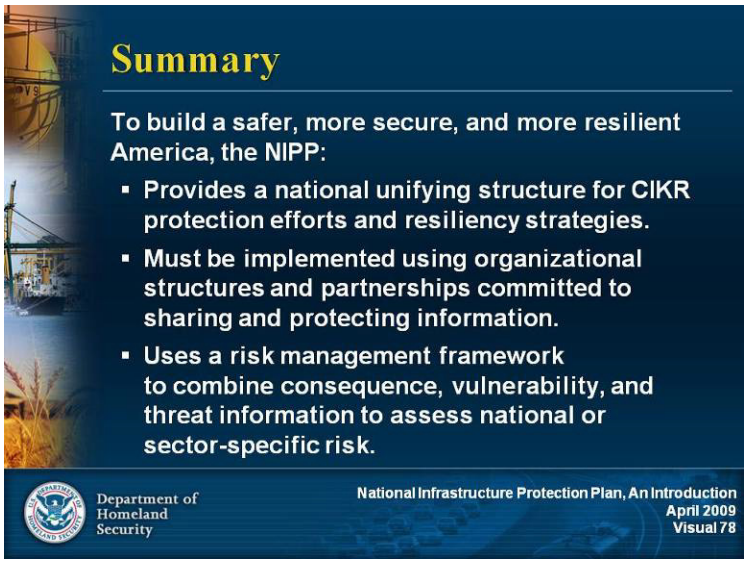
Instructor Notes

To ensure an effective, efficient CIKR protection program over the long term, the following key activities are needed:

- **Building national awareness** to support the CIKR protection program and related investments.
- **Enabling education, training, and exercise programs** to ensure that skilled and knowledgeable professionals and experienced organizations are able to undertake NIPP-related responsibilities.
- **Conducting research and development (R&D) and using technology** to improve CIKR protective capabilities or resiliency strategies or to lower the costs of existing capabilities.
- **Developing, protecting, and maintaining data systems and simulations** to enable continuously refined risk assessment within and across sectors and to ensure preparedness.
- **Continuously improving the NIPP** and associated plans and programs through ongoing management and revision, as required.

Topic The Long-Term Vision

Visual 78



Visual Description: Summary

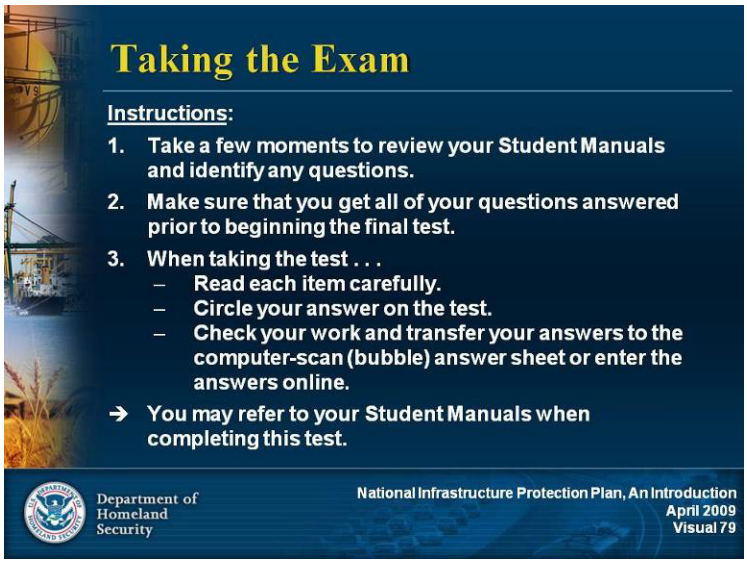
Instructor Notes

Summarize the course by presenting the following key points:

- The overarching goal of the NIPP is to build a safer, more secure, and more resilient America by preventing, deterring, neutralizing, or mitigating the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit elements of our Nation's CIKR, and to strengthen national preparedness, timely response, and rapid recovery of CIKR in the event of an attack, natural disaster, or other emergency.
- Protecting the critical infrastructure and key resources of the United States is essential to the Nation's security, public health and safety, economic vitality, and way of life.
- The NIPP provides the unifying structure for the integration of existing and future critical infrastructure and key resources (CIKR) protection efforts and resiliency strategies into a single national program.
- 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. DHS, in close collaboration with the SSAs, is responsible for overall coordination of the NIPP partnership organization and information-sharing network.
- The cornerstone of the NIPP is its risk management framework, which establishes the process for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector-specific risk that promote continuous improvement to enhance CIKR protection.
- Successful implementation of the NIPP relies on information sharing at all levels. The NIPP complements other homeland security plans and strategies such as the National Response Framework.
- The NIPP information-sharing approach uses a networked model, allowing distribution and access to information both vertically and horizontally, as well as the ability to enable decentralized decisionmaking and actions.

Topic | **The Long-Term Vision**

Visual 79



Visual Description: Taking the Exam

Instructor Notes

Provide the following instructions to the participants:

1. Take a few moments to review your Student Manuals and identify any questions.

2. Make sure that you get all of your questions answered prior to beginning the Final Test.

3. When taking the test . . .
   - Read each item carefully.
   - Circle your answer on the test.
   - Check your work and transfer your answers to the computer-scan (bubble) answer sheet or enter the answers online.

4. Refer to your Student Manuals or the NIPP as needed when completing this test.

Instructor Note Regarding Review: It is important that you allow the participants enough time to review the course materials prior to taking the exam. If time permits, you can facilitate a structured review of the materials.

Answer the participants' review questions. After all the questions have been answered, tell the participants that you will be distributing the Final Test.

Ask the participants to complete the test. Collect all tests when finished.

Topic | **The Long-Term Vision**

Visual 80

Visual Description: Feedback

Instructor Notes

Distribute the course evaluation forms. Ask the participants to complete the evaluation. After the class completes the evaluations, ask for comments on the strengths of the course and areas for improvement. Thank the participants for attending this training.

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

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

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

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

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

Cybersecurity: The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure the information's confidentiality, integrity, and availability. Includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems.

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

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

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

Infrastructure: The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole. Consistent with the definition in the Homeland Security Act, infrastructure includes physical, cyber, and/or human elements.

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

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

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

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

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

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

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

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

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

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

Risk: The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.

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

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

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

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

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

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

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

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

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

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

Resource | **Acronyms**

CIKR: Critical Infrastructure and Key Resources

CIPAC: Critical Infrastructure Partnership Advisory Council

COI: Community of Interest

DHS: Department of Homeland Security

FSLC: Federal Senior Leadership Council

GCC: Government Coordinating Council

HSAC: Homeland Security Advisory Council

HSIN: Homeland Security Information Network

HSPD: Homeland Security Presidential Directive

IC: Intelligence Community

IT: Information Technology

NIAC: National Infrastructure Advisory Council

NIMS: National Incident Management System

NIPP: National Infrastructure Protection Plan

NRF: National Response Framework

NS/EP: National Security and Emergency Preparedness

NSTAC: National Security Telecommunications Advisory Committee

PCII: Protected Critical Infrastructure Information

PCIS: Partnership for Critical Infrastructure Security

PVTSAC: Private Sector Senior Advisory Committee

SCC: Sector Coordinating Council

SLTGCC: State, Local, and Tribal Government Coordinating Council

SSA: Sector-Specific Agency

SSP: Sector-Specific Plan