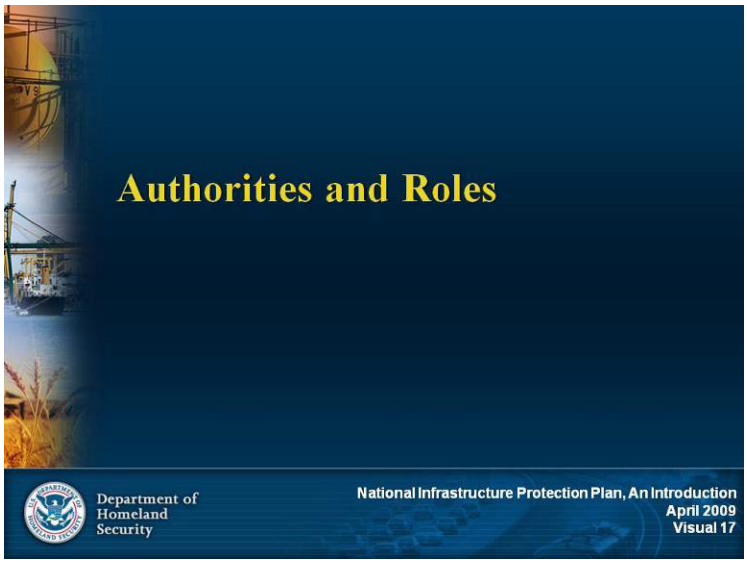
Topic | **Authorities and Roles**

Visual 17



Visual Description: Authorities and Roles

Instructor Notes

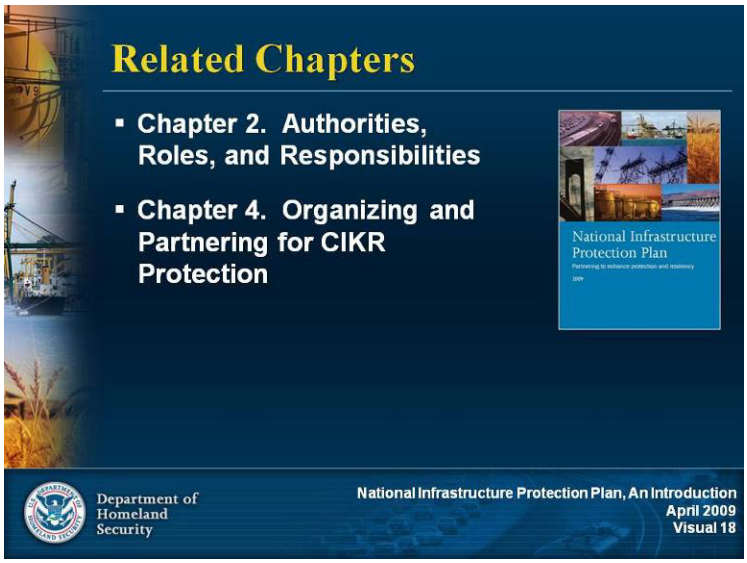
Given the complex threats we face, it is incumbent upon the Federal Government to provide overarching leadership and coordination in the CIKR protection mission area. To that end, the Government has created several authorities that give NIPP participants the authority to protect the CIKR under their supervision.

Protection of CIKR also is managed through collaboration between NIPP participants, and the assigning of specific roles.

This section of the course discusses the authorities, roles, and partnerships that, as part of the NIPP, protect CIKR.

Topic | **Authorities and Roles**

Visual 18



Visual Description: Related Chapters

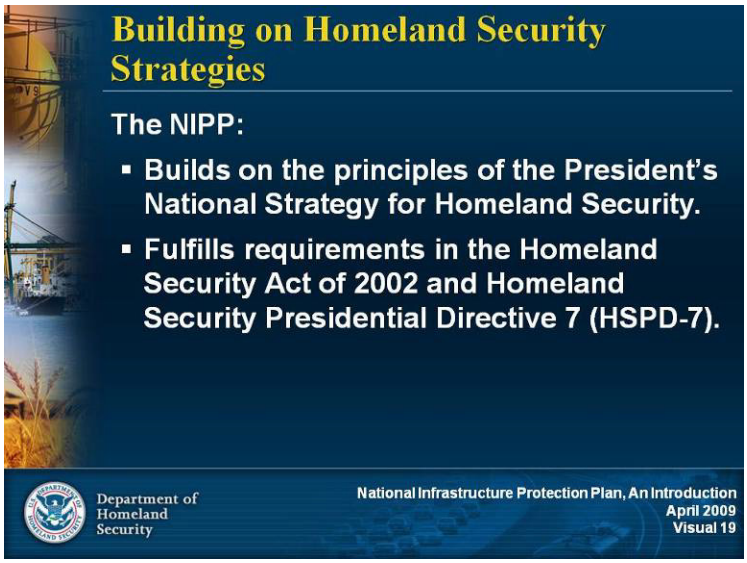
Instructor Notes

This section summarizes the information presented in the following chapters of the NIPP:

- Chapter 2. Authorities, Roles, and Responsibilities
- Chapter 4. Organizing and Partnering for CIKR Protection

Topic | **Authorities**

Visual 19



Visual Description: Building on Homeland Security Strategies

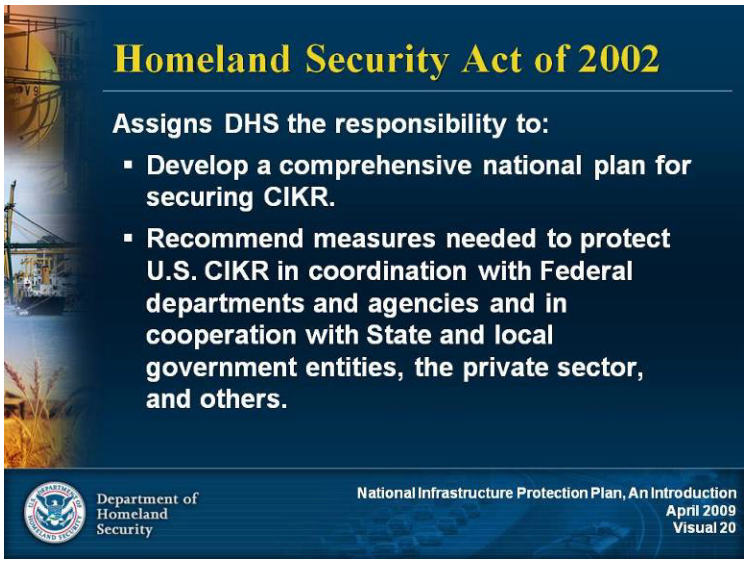
Instructor Notes

The NIPP formalizes and strengthens existing CIKR partnerships and creates the baseline for how the public and private sectors will work together. In addition, the NIPP:

- Builds on the principles of the President's National Strategy for Homeland Security and its companion strategies for the physical protection of critical infrastructure and key assets and the securing of cyberspace.
- Fulfills requirements in the Homeland Security Act of 2002 and Homeland Security Presidential Directive 7 (HSPD-7).

Topic | **Authorities**

Visual 20



Visual Description: Homeland Security Act of 2002

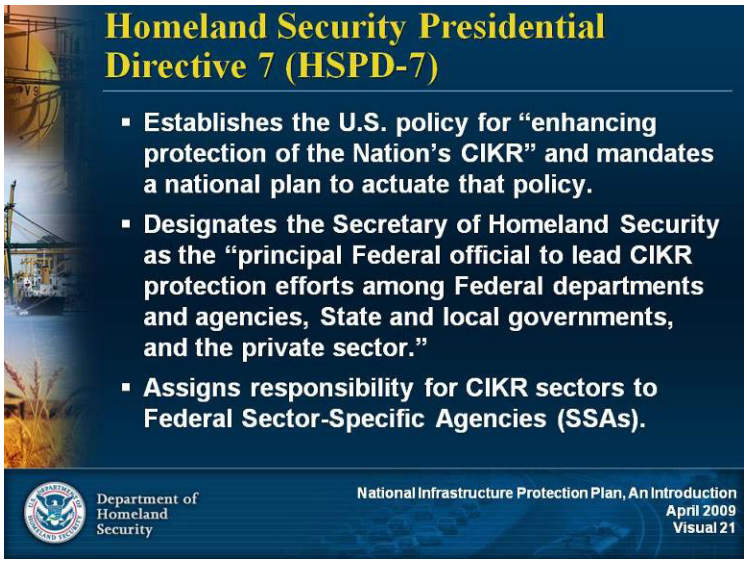
Instructor Notes

The Homeland Security Act of 2002 provides the primary authority for the overall homeland security mission and provides the basis for Department of Homeland Security (DHS) responsibilities in the protection of the Nation's CIKR.

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

Topic | **Authorities**

Visual 21



Visual Description: Homeland Security Presidential Directive 7 (HSPD-7)

Instructor Notes

The national approach for CIKR protection is provided through the unifying framework established in HSPD-7. This directive establishes the U.S. policy for enhancing protection of the Nation's CIKR and mandates a national plan to actuate that policy.

In HSPD-7, the President designated the Secretary of Homeland Security as the principal Federal official to lead CIKR protection efforts among Federal departments and agencies, State and local governments, and the private sector and assigns responsibility for CIKR sectors to Federal Sector-Specific Agencies (SSAs).

The full text of HSPD-7 appears on the following pages.

Homeland Security Presidential Directive/HSPD-7

Subject: Critical Infrastructure Identification, Prioritization, and Protection

Purpose

(1) This directive establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.

Background

(2) Terrorists seek to destroy, incapacitate, or exploit critical infrastructure and key resources across the United States to threaten national security, cause mass casualties, weaken our economy, and damage public morale and confidence.

(3) America's open and technologically complex society includes a wide array of critical infrastructure and key resources that are potential terrorist targets. The majority of these are owned and operated by the private sector and State or local governments. These critical infrastructures and key resources are both physical and cyber-based and span all sectors of the economy.

(4) Critical infrastructure and key resources provide the essential services that underpin American society. The Nation possesses numerous key resources, whose exploitation or destruction by terrorists could cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction, or could profoundly affect our national prestige and morale. In addition, there is critical infrastructure so vital that its incapacitation, exploitation, or destruction, through terrorist attack, could have a debilitating effect on security and economic well-being.

(5) While it is not possible to protect or eliminate the vulnerability of all critical infrastructure and key resources throughout the country, strategic improvements in security can make it more difficult for attacks to succeed and can lessen the impact of attacks that may occur. In addition to strategic security enhancements, tactical security improvements can be rapidly implemented to deter, mitigate, or neutralize potential attacks.

Definitions

(6) In this directive:

(a) The term “critical infrastructure” has the meaning given to that term in section 1016(e) of the USA PATRIOT Act of 2001 (42 U.S.C. 5195c(e)).

(b) The term “key resources” has the meaning given that term in section 2(9) of the Homeland Security Act of 2002 (6 U.S.C. 101(9)).

(c) The term “the Department” means the Department of Homeland Security.

(d) The term “Federal departments and agencies” means those executive departments enumerated in 5 U.S.C. 101, and the Department of Homeland Security; independent establishments as defined by 5 U.S.C. 104(1); Government corporations as defined by 5 U.S.C. 103(1); and the United States Postal Service.

(e) The terms “State,” and “local government,” when used in a geographical sense, have the same meanings given to those terms in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101).

(f) The term “the Secretary” means the Secretary of Homeland Security.

(g) The term “Sector-Specific Agency” means a Federal department or agency responsible for infrastructure protection activities in a designated critical infrastructure sector or key resources category. Sector-Specific Agencies will conduct their activities under this directive in accordance with guidance provided by the Secretary.

(h) The terms “protect” and “secure” mean reducing the vulnerability of critical infrastructure or key resources in order to deter, mitigate, or neutralize terrorist attacks.

Policy

(7) It is the policy of the United States to enhance the protection of our Nation's critical infrastructure and key resources against terrorist acts that could:

(a) cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction;

(b) impair Federal departments and agencies' abilities to perform essential missions, or to ensure the public's health and safety;

(c) undermine State and local government capacities to maintain order and to deliver minimum essential public services;

(d) damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services;

(e) have a negative effect on the economy through the cascading disruption of other critical infrastructure and key resources; or

(f) undermine the public's morale and confidence in our national economic and political institutions.

(8) Federal departments and agencies will identify, prioritize, and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them. Federal departments and agencies will work with State and local governments and the private sector to accomplish this objective.

(9) Federal departments and agencies will ensure that homeland security programs do not diminish the overall economic security of the United States.

(10) Federal departments and agencies will appropriately protect information associated with carrying out this directive, including handling voluntarily provided information and information that would facilitate terrorist targeting of critical infrastructure and key resources consistent with the Homeland Security Act of 2002 and other applicable legal authorities.

(11) Federal departments and agencies shall implement this directive in a manner consistent with applicable provisions of law, including those protecting the rights of United States persons.

Roles and Responsibilities of the Secretary

(12) In carrying out the functions assigned in the Homeland Security Act of 2002, the Secretary shall be responsible for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States. The Secretary shall serve as the principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources.

(13) Consistent with this directive, the Secretary will identify, prioritize, and coordinate the protection of critical infrastructure and key resources with an emphasis on critical infrastructure and key resources that could be exploited to cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction.

(14) The Secretary will establish uniform policies, approaches, guidelines, and methodologies for integrating Federal infrastructure protection and risk management activities within and across sectors along with metrics and criteria for related programs and activities.

(15) The Secretary shall coordinate protection activities for each of the following critical infrastructure sectors: information technology; telecommunications; chemical; transportation systems, including mass

transit, aviation, maritime, ground/surface, and rail and pipeline systems; emergency services; and postal and shipping. The Department shall coordinate with appropriate departments and agencies to ensure the protection of other key resources including dams, government facilities, and commercial facilities. In addition, in its role as overall cross-sector coordinator, the Department shall also evaluate the need for and coordinate the coverage of additional critical infrastructure and key resources categories over time, as appropriate.

(16) The Secretary will continue to maintain an organization to serve as a focal point for the security of cyberspace. The organization will facilitate interactions and collaborations between and among Federal departments and agencies, State and local governments, the private sector, academia and international organizations. To the extent permitted by law, Federal departments and agencies with cyber expertise, including but not limited to the Departments of Justice, Commerce, the Treasury, Defense, Energy, and State, and the Central Intelligence Agency, will collaborate with and support the organization in accomplishing its mission. The organization's mission includes analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems. The organization will support the Department of Justice and other law enforcement agencies in their continuing missions to investigate and prosecute threats to and attacks against cyberspace, to the extent permitted by law.

(17) The Secretary will work closely with other Federal departments and agencies, State and local governments, and the private sector in accomplishing the objectives of this directive.

Roles and Responsibilities of Sector-Specific Federal Agencies

(18) Recognizing that each infrastructure sector possesses its own unique characteristics and operating models, there are designated Sector-Specific Agencies, including:

(a) Department of Agriculture -- agriculture, food (meat, poultry, egg products);

(b) Health and Human Services -- public health, healthcare, and food (other than meat, poultry, egg products);

(c) Environmental Protection Agency -- drinking water and water treatment systems;

(d) Department of Energy -- energy, including the production refining, storage, and distribution of oil and gas, and electric power except for commercial nuclear power facilities;

(e) Department of the Treasury -- banking and finance;

(f) Department of the Interior -- national monuments and icons; and

(g) Department of Defense -- defense industrial base.

(19) In accordance with guidance provided by the Secretary, Sector-Specific Agencies shall:

(a) collaborate with all relevant Federal departments and agencies, State and local governments, and the private sector, including with key persons and entities in their infrastructure sector;

(b) conduct or facilitate vulnerability assessments of the sector; and

(c) encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources.

(20) Nothing in this directive alters, or impedes the ability to carry out, the authorities of the Federal departments and agencies to perform their responsibilities under law and consistent with applicable legal authorities and presidential guidance.

(21) Federal departments and agencies shall cooperate with the Department in implementing this directive, consistent with the Homeland Security Act of 2002 and other applicable legal authorities.

Roles and Responsibilities of Other Departments, Agencies, and Offices

(22) In addition to the responsibilities given the Department and Sector-Specific Agencies, there are special functions of various Federal departments and agencies and components of the Executive Office of the President related to critical infrastructure and key resources protection.

(a) The Department of State, in conjunction with the Department, and the Departments of Justice, Commerce, Defense, the Treasury and other appropriate agencies, will work with foreign countries and international organizations to strengthen the protection of United States critical infrastructure and key resources.

(b) The Department of Justice, including the Federal Bureau of Investigation, will reduce domestic terrorist threats, and investigate and prosecute actual or attempted terrorist attacks on, sabotage of, or disruptions of critical infrastructure and key resources. The Attorney General and the Secretary shall use applicable statutory authority and attendant mechanisms for cooperation and coordination, including but not limited to those established by presidential directive.

(c) The Department of Commerce, in coordination with the Department, will work with private sector, research, academic, and government organizations to improve technology for cyber systems and promote other critical infrastructure efforts, including using its authority under the Defense Production Act to assure the timely availability of industrial products, materials, and services to meet homeland security requirements.

(d) A Critical Infrastructure Protection Policy Coordinating Committee will advise the Homeland Security Council on interagency policy related to physical and cyber infrastructure protection. This PCC will be chaired by a Federal officer or employee designated by the Assistant to the President for Homeland Security.

(e) The Office of Science and Technology Policy, in coordination with the Department, will coordinate interagency research and development to enhance the protection of critical infrastructure and key resources.

(f) The Office of Management and Budget (OMB) shall oversee the implementation of government-wide policies, principles, standards, and guidelines for Federal government computer security programs. The Director of OMB will ensure the operation of a central Federal information security incident center consistent with the requirements of the Federal Information Security Management Act of 2002.

(g) Consistent with the E-Government Act of 2002, the Chief Information Officers Council shall be the principal interagency forum for improving agency practices related to the design, acquisition, development, modernization, use, operation, sharing, and performance of information resources of Federal departments and agencies.

(h) The Department of Transportation and the Department will collaborate on all matters relating to transportation security and transportation infrastructure protection. The Department of Transportation is responsible for operating the national air space system. The Department of Transportation and the Department will collaborate in regulating the transportation of hazardous materials by all modes (including pipelines).

(i) All Federal departments and agencies shall work with the sectors relevant to their responsibilities to reduce the consequences of catastrophic failures not caused by terrorism.

(23) The heads of all Federal departments and agencies will coordinate and cooperate with the Secretary as appropriate and consistent with their own responsibilities for protecting critical infrastructure and key resources.

(24) All Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and protection of their respective internal critical infrastructure and key resources. Consistent with the Federal Information Security Management Act of 2002, agencies will identify and provide information security protections commensurate with the risk and magnitude of the

harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

Coordination with the Private Sector

(25) In accordance with applicable laws or regulations, the Department and the Sector-Specific Agencies will collaborate with appropriate private sector entities and continue to encourage the development of information sharing and analysis mechanisms. Additionally, the Department and Sector-Specific Agencies shall collaborate with the private sector and continue to support sector-coordinating mechanisms:

(a) to identify, prioritize, and coordinate the protection of critical infrastructure and key resources; and

(b) to facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices.

National Special Security Events

(26) The Secretary, after consultation with the Homeland Security Council, shall be responsible for designating events as "National Special Security Events" (NSSEs). This directive supersedes language in previous presidential directives regarding the designation of NSSEs that is inconsistent herewith.

Implementation

(27) Consistent with the Homeland Security Act of 2002, the Secretary shall produce a comprehensive, integrated National Plan for Critical Infrastructure and Key Resources Protection to outline national goals, objectives, milestones, and key initiatives within 1 year from the issuance of this directive. The Plan shall include, in addition to other Homeland Security-related elements as the Secretary deems appropriate, the following elements:

(a) a strategy to identify, prioritize, and coordinate the protection of critical infrastructure and key resources, including how the Department intends to work with Federal departments and agencies, State and local governments, the private sector, and foreign countries and international organizations;

(b) a summary of activities to be undertaken in order to: define and prioritize, reduce the vulnerability of, and coordinate the protection of critical infrastructure and key resources;

(c) a summary of initiatives for sharing critical infrastructure and key resources information and for providing critical infrastructure and key resources threat warning data to State and local governments and the private sector; and

(d) coordination and integration, as appropriate, with other Federal emergency management and preparedness activities including the National Response Framework and applicable national preparedness goals.

(28) The Secretary, consistent with the Homeland Security Act of 2002 and other applicable legal authorities and presidential guidance, shall establish appropriate systems, mechanisms, and procedures to share homeland security information relevant to threats and vulnerabilities in national critical infrastructure and key resources with other Federal departments and agencies, State and local governments, and the private sector in a timely manner.

(29) The Secretary will continue to work with the Nuclear Regulatory Commission and, as appropriate, the Department of Energy in order to ensure the necessary protection of:

(a) commercial nuclear reactors for generating electric power and non-power nuclear reactors used for research, testing, and training;

(b) nuclear materials in medical, industrial, and academic settings and facilities that fabricate nuclear fuel; and

(c) the transportation, storage, and disposal of nuclear materials and waste.

(30) In coordination with the Director of the Office of Science and Technology Policy, the Secretary shall prepare on an annual basis a Federal Research and Development Plan in support of this directive.

(31) The Secretary will collaborate with other appropriate Federal departments and agencies to develop a program, consistent with applicable law, to geospatially map, image, analyze, and sort critical infrastructure and key resources by utilizing commercial satellite and airborne systems, and existing capabilities within other agencies. National technical means should be considered as an option of last resort. The Secretary, with advice from the Director of Central Intelligence, the Secretaries of Defense and the Interior, and the heads of other appropriate Federal departments and agencies, shall develop mechanisms for accomplishing this initiative. The Attorney General shall provide legal advice as necessary.

(32) The Secretary will utilize existing, and develop new, capabilities as needed to model comprehensively the potential implications of terrorist exploitation of vulnerabilities in critical infrastructure and key resources, placing specific focus on densely populated areas. Agencies with relevant modeling capabilities shall cooperate with the Secretary to develop appropriate mechanisms for accomplishing this initiative.

(33) The Secretary will develop a national indications and warnings architecture for infrastructure protection and capabilities that will facilitate:

(a) an understanding of baseline infrastructure operations;

(b) the identification of indicators and precursors to an attack; and

(c) a surge capacity for detecting and analyzing patterns of potential attacks.

In developing a national indications and warnings architecture, the Department will work with Federal, State, local, and non-governmental entities to develop an integrated view of physical and cyber infrastructure and key resources.

(34) By July 2004, the heads of all Federal departments and agencies shall develop and submit to the Director of the OMB for approval plans for protecting the physical and cyber critical infrastructure and key resources that they own or operate. These plans shall address identification, prioritization, protection, and contingency planning, including the recovery and reconstitution of essential capabilities.

(35) On an annual basis, the Sector-Specific Agencies shall report to the Secretary on their efforts to identify, prioritize, and coordinate the protection of critical infrastructure and key resources in their respective sectors. The report shall be submitted within 1 year from the issuance of this directive and on an annual basis thereafter.

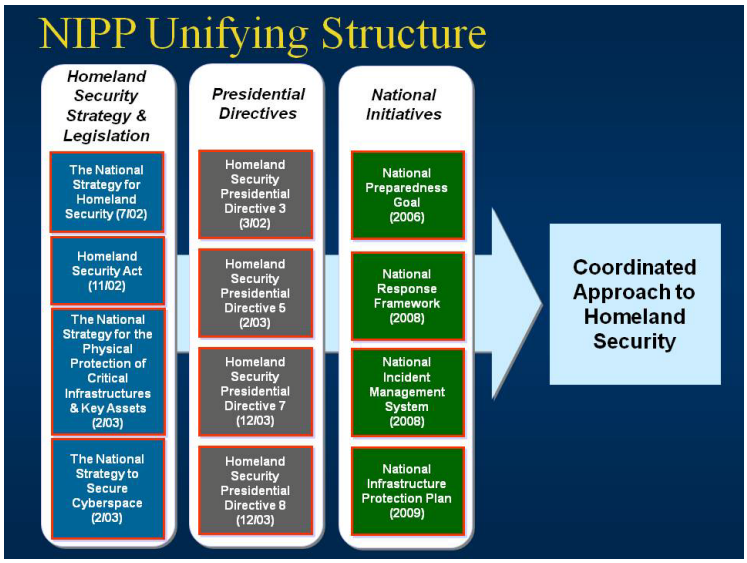
(36) The Assistant to the President for Homeland Security and the Assistant to the President for National Security Affairs will lead a national security and emergency preparedness communications policy review, with the heads of the appropriate Federal departments and agencies, related to convergence and next generation architecture. Within 6 months after the issuance of this directive, the Assistant to the President for Homeland Security and the Assistant to the President for National Security Affairs shall submit for my consideration any recommended changes to such policy.

(37) This directive supersedes Presidential Decision Directive/NSC-63 of May 22, 1998 ("Critical Infrastructure Protection"), and any Presidential directives issued prior to this directive to the extent of any inconsistency. Moreover, the Assistant to the President for Homeland Security and the Assistant to the President for National Security Affairs shall jointly submit for my consideration a Presidential directive to make changes in Presidential directives issued prior to this date that conform such directives to this directive.

(38) This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

Topic | **Authorities**

Visual 22



Visual Description: NIPP Unifying Structure

Instructor Notes

The NIPP was built on a series of national policy documents that used a risk management framework to foster a more secure environment for the Nation's citizens and critical infrastructure. These authorities created a strategy for using America's talents and resources to enhance our protection and reduce our vulnerability to terrorist attacks. The result is a coordinated approach to homeland security that integrates mandates from:

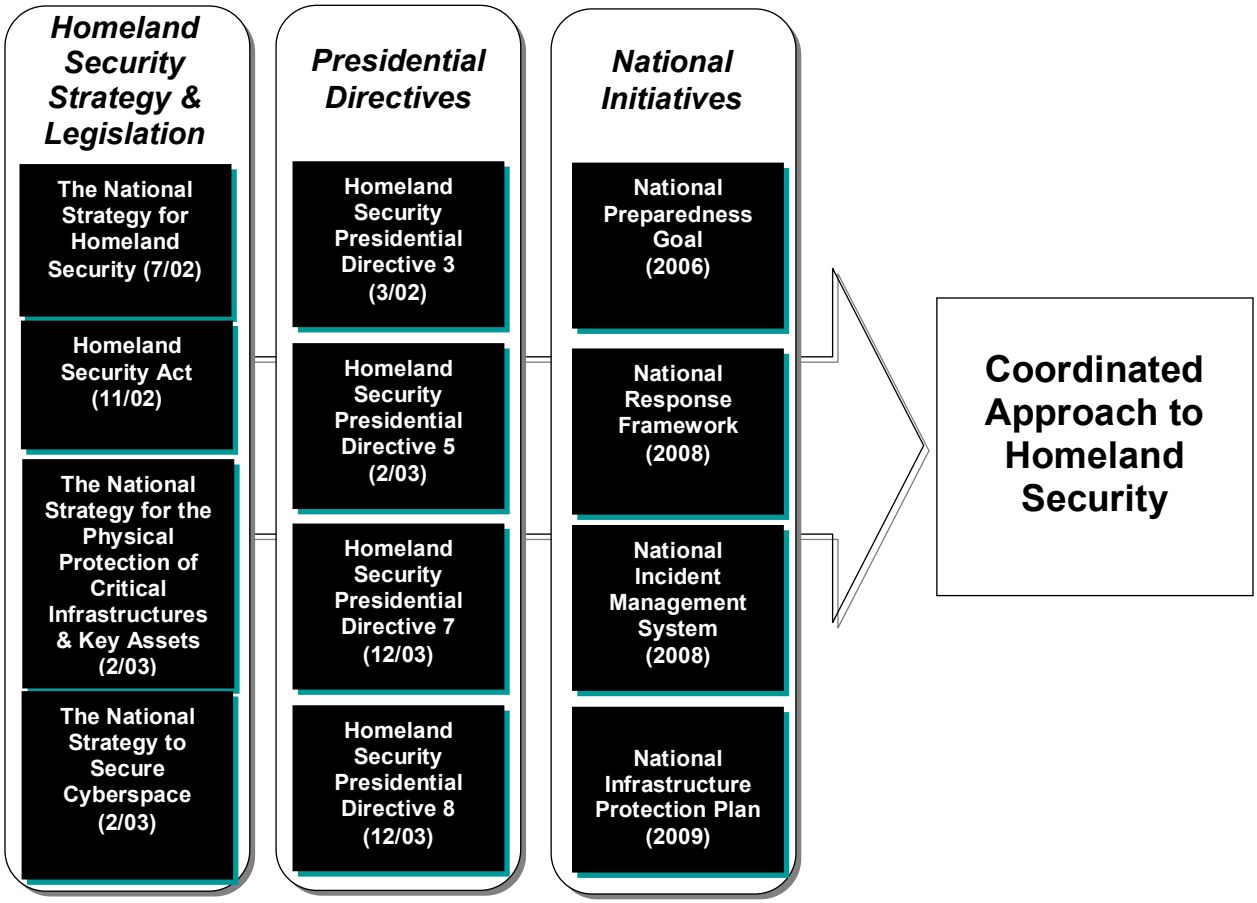
- **Homeland Security Strategy and Legislation.** The following documents define the mission, structure, and operations of the Department of Homeland Security:
  - The National Strategy for Homeland Security
  - The Homeland Security Act
  - The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets
  - The National Strategy to Secure Cyberspace

- **Presidential Directives.** The following HSPDs provide direction:
  - HSPD-3: Homeland Security Advisory System
  - HSPD-5: Management of Domestic Incidents
  - HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection
  - HSPD-8: National Preparedness

- **National Initiatives.** The national initiatives include:
  - National Preparedness Goal
  - National Response Framework
  - National Incident Management System
  - National Infrastructure Protection Plan

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

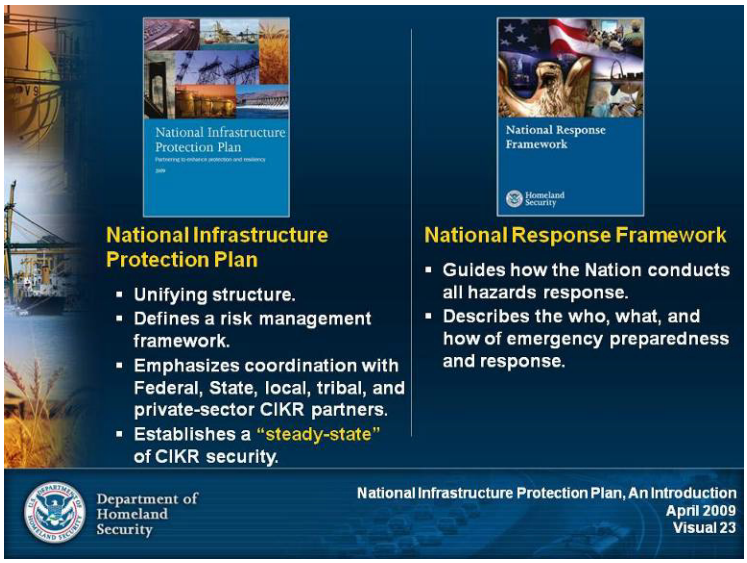
Topic Authorities



Caption: Graphic showing the strategies and other authorities that support NIPP's unifying structure and its coordinated approach to homeland security.

Topic | **Roles**

Visual 23



Visual Description: NIPP/NRF

Instructor Notes

To be effective, the NIPP must complement:

- Homeland security plans and strategies at the Federal, State, local, and tribal levels of government that address CIKR protection within their respective jurisdictions.
- Business continuity plans and resilience measures and other CIKR protection-related plans and programs instituted by the private sector.

The NIPP and the National Response Framework (NRF) work together to provide a comprehensive, integrated approach to the homeland security mission:

- The NIPP and its associated SSPs establish the Nation's steady-state level of protection by helping to focus resources where investment yields the greatest return in terms of national risk management.
- The NRF addresses response and short-term recovery in the context of domestic threat and incident management.

The NIPP risk management framework, partnership model, and information-sharing mechanisms are structured to support coordination and cooperation between the public and private sectors and provide for smooth transitions from steady-state operations to incident response.

The CIKR Support Annex to the NRF:

- Provides a bridge between the NIPP steady-state CIKR protection and the NRF incident management.
- Provides processes for integrating the CIKR perspective as a key component of domestic incident management.
- Applies NIPP processes for situational awareness, assessment, and information sharing to augment incident management processes.
- Provides focus on sector and cross-sector impacts, and cascading effects.

Topic | **Activity**

Visual 24

Visual Description: Activity: NIPP Applicability

Instructor Notes

Ask the participants to answer the following question:

Which of the following events or activities are within the scope of the NIPP authorities?

1. Attack on a military installation
2. Power blackout affecting the Northwest region
3. Response to localized flooding
4. Continuity of operations planning
5. Disruption of major agricultural product processing plants
6. Overseas bombing of a U.S. Embassy
7. Cyber attack on domestic banking systems

If necessary, note that the correct answers are 2, 4, 5, and 7.

Topic	Roles

Visual 25

Visual Description: Sector-Specific Agency (SSA) Roles

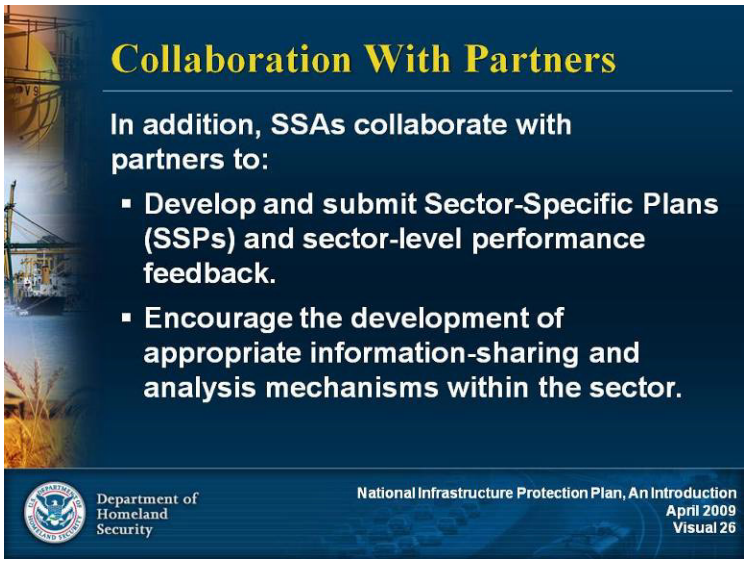
Instructor Notes

HSPD-7 designated responsibility to various Federal Government departments and agencies to serve as SSAs for each of the CIKR sectors.

Sector-Specific Agencies (SSAs) are responsible for working with DHS and their respective Government Coordinating Councils to: implement the NIPP sector partnership model and risk management framework; develop protective programs, resiliency strategies, and related requirements; and provide sector-level CIKR protection guidance in line with the overarching guidance.

Topic | **Roles**

Visual 26



Visual Description: Collaboration With Partners

Instructor Notes

In addition, SSAs collaborate with partners to:

- Develop and submit Sector-Specific Plans (SSPs) and sector-level performance feedback.
- Encourage the development of appropriate information-sharing and analysis mechanisms within the sector.

Topic	Roles

Visual 27

Visual Description: Private Sector Responsibilities

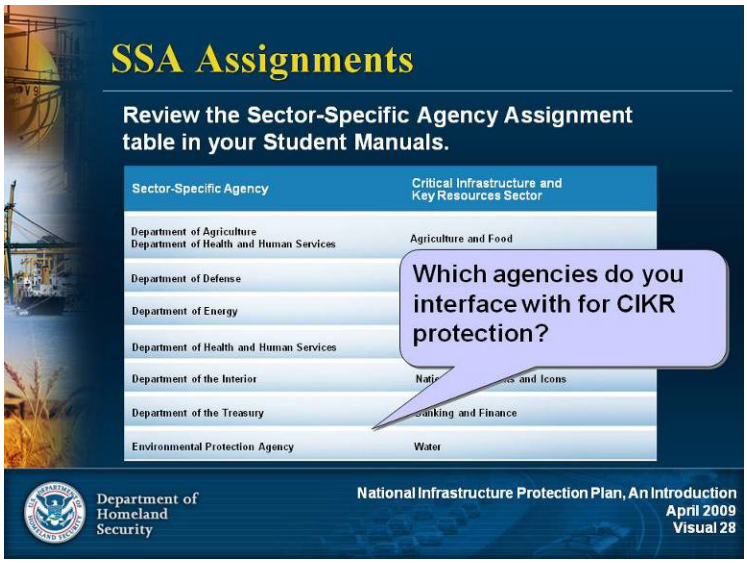
Instructor Notes

The private sector is responsible for the following:

- Management of a vast majority of CIKR in most sectors.
- Knowledge of CIKR assets, systems, networks, functions, and other capabilities.
- Taking action to reduce risk and respond to and recover from incidents.
- Providing products, services, and technologies to address security gaps.
- Sharing and protecting sensitive information regarding threats, vulnerabilities, consequences, countermeasures, and best practices.

Topic | **Roles**

Visual 28



Visual Description: SSA Assignments

Instructor Notes

Review the 18 CIKR sectors and designated Federal Government SSAs in HSPD-7, which are outlined in the table on the next page.

Topic | **Roles**

Sector-Specific Agency	CIKR Sector
Department of Agriculture[1] Department of Health and Human Services[2]	Agriculture and Food
Department of Defense[3]	Defense Industrial Base
Department of Energy	Energy[4]
Department of Health and Human Services	Healthcare and Public Health
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Water[5]
Department of Homeland Security *Office of Infrastructure Protection*	Chemical Commercial Facilities Critical Manufacturing Dams Emergency Services Nuclear Reactors, Materials, and Waste
Office of Cybersecurity and Telecommunications	Information Technology Communications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration, U.S. Coast Guard[6]	Transportation Systems[7]
Immigration and Customs Enforcement, Federal Protective Service	Government Facilities[8]

1. The Department of Agriculture is responsible for agriculture and food (meat, poultry, and egg products).
2. The Department of Health and Human Services is responsible for food other than meat, poultry, and egg products.
3. Nothing in this plan impairs or otherwise affects the authority of the Secretary of Defense over the Department of Defense (DOD), including the chain of command for military forces from the President as Commander in Chief, to the Secretary of Defense, to the commander of military forces, or military command and control procedures.
4. The Energy Sector includes the production, refining, storage, and distribution of oil, gas, and electric power, except for nuclear power facilities.
5. The Water Sector includes drinking water and wastewater systems.
6. The U.S. Coast Guard is the SSA for the maritime transportation mode.
7. As stated in HSPD-7, the Department of Transportation and the Department of Homeland Security will collaborate on all matters relating to transportation security and transportation infrastructure protection.
8. The Department of Education is the SSA for the Education Facilities Subsector of the Government Facilities Sector.

Topic | **Roles**

Visual 29

Visual Description: Other Federal Agencies

Instructor Notes

All Federal departments and agencies function as CIKR partners. Federal departments and agencies that are not designated as SSAs but have unique responsibilities, functions, or expertise in a particular CIKR sector:

- Assist in identifying and assessing high-consequence CIKR and enabling protective actions and programs within that sector.
- Support the national goal of enhancing CIKR protection through their role as the regulatory agency for owners and operators represented within a specific sector when so designated by statute.
- Collaborate with all relevant security partners to share security-related information within the sector, as appropriate.

The chart on the following page outlines the responsibilities from the NIPP for other Federal departments.

Topic **Roles**

Department	Responsibility
Department of State *(in coordination with DHS and the Departments of Justice, Commerce, Defense, and Treasury)*	Works with foreign governments and international organizations to strengthen U.S. CIKR protection efforts.
Department of Justice *(in coordination with DHS)*	Acts to reduce terrorist threats, and investigates and prosecutes actual or attempted attacks on, sabotage of, or disruptions of CIKR.
Department of Commerce *(in coordination with DHS, the private sector, and research, academic, and government organizations)*	Improves technology for cyber systems and promotes other critical infrastructure efforts, including using its authority under the Defense Production Act to ensure the timely availability of industrial products, materials, and services to meet homeland security requirements.
Department of Transportation (DOT) *(in coordination with DHS)*	Works on all matters related to transportation security and transportation infrastructure protection, and is additionally responsible for operating the National Airspace System. Regulates the transportation of hazardous materials by all modes (including pipelines).
Nuclear Regulatory Commission (NRC) *(in coordination with DHS and the Department of Energy)*	Works to ensure the protection of nuclear reactors for generating electric power and nonpower nuclear reactors used for research, testing, and training; nuclear materials in medical, industrial, and academic settings and facilities that fabricate nuclear fuel; and the transportation, storage, and disposal of nuclear materials and waste.

Topic | **Roles**

Visual 30

Visual Description: State, Local, Tribal, and Territorial Governments

Instructor Notes

State, local, tribal, and territorial governments are responsible for implementing the homeland security mission, protecting public safety and welfare, and ensuring the provision of essential services to communities and industries within their jurisdictions.

- **State and Territorial Governments.**
  - Serve as crucial coordination hubs, bringing together prevention, protection, response, and recovery authorities, capacities, and resources.
  - Coordinate requests for Federal assistance when the threat or incident situation exceeds jurisdictional capabilities.
  - Develop and implement statewide/regional CIKR protection programs that reflect the full range of NIPP-related activities.
  - Facilitate the information-sharing process. States receive CIKR information from the Federal Government to support the national and State CIKR protection programs.
- **Local Governments.** Local governments represent the frontlines for homeland security and, more specifically, for CIKR protection and implementation of the NIPP. Local governments:
  - Provide critical public services and functions in conjunction with private sector owners and operators. In some sectors, local government entities own and operate CIKR such as water, stormwater, and electric utilities.
  - Drive emergency preparedness, as well as local participation in NIPP and SSP implementation, across a variety of jurisdictional security partners.

Topic | **Roles**

- **Tribal Governments.** Tribal government roles and responsibilities regarding CIKR protection generally mirror those of State and local governments. Tribal governments are accountable for the public health, welfare, and safety of tribal members, as well as the protection of CIKR and continuity of essential services under their jurisdiction.

  Under the NIPP partnership model, tribal governments must ensure coordination with Federal, State, local, and international counterparts to achieve synergy in the implementation of the NIPP and SSP frameworks.

Topic | **Roles**

Visual 31

Visual Description: Regional Partners

Instructor Notes

Regional security partnerships include a variety of public-private initiatives that cross jurisdictional and/or sector boundaries and focus on homeland security preparedness, protection, response, and recovery within or serving the population of a defined geographical area.

Specific regional initiatives range in scope from organizations that include multiple jurisdictions and private sector partners within a single State, to groups that involve jurisdictions and enterprises in more than one State and across international borders. In many cases, State governments also collaborate through the adoption of interstate compacts to formalize regionally based partnerships regarding CIKR protection.

The Pacific NorthWest Economic Region provides an example of a regional organization structured as a public-private partnership that includes legislators, governments, and businesses in five States and three Canadian Provinces.

The Region, established by statute in all member States and Provinces:

- Sponsors binational, multijurisdictional CIKR protection interdependency exercises.
- Has developed an action plan outlining several physical and cyber CIKR protection projects with important regional impact.

Topic | **Roles**

Visual 32

Visual Description: International Coordination

Instructor Notes

- The NIPP addresses international CIKR protection, including interdependencies and vulnerabilities based on threats that originate outside the country or transit through it.
- The U.S. Government and the private sector work with foreign governments and international/multinational organizations to enhance the confidentiality, integrity, and availability of cyber infrastructures and products.
- Protection of assets, systems, and networks that operate across or near the borders with Canada and Mexico, or rely on other international aspects to enable critical functionality, requires coordination with, and planning and/or sharing resources among, neighboring governments at all levels, as well as private sector CIKR owners and operators.
- The U.S. Government and private sector corporations have a significant number of facilities located outside of the United States that may be considered CIKR.
- Special consideration is required when CIKR is extensively integrated into an international or global market (e.g., financial services, agriculture, energy, transportation, telecommunications, or information technology) or when a sector relies on inputs that are not within the control of U.S. entities.
- Special consideration is required when government facilities and functions are directly affected by foreign owned and operated commercial facilities.

Topic Roles

Visual 33

Visual Description: Boards, Commissions, Authorities, Councils, and Other Entities

Instructor Notes

Boards, commissions, authorities, councils, and other entities at all levels perform regulatory, advisory, policy, or business oversight functions related to various aspects of CIKR operations and protection within and across sectors and jurisdictions.

Examples of these groups include, but are not limited to: transportation authorities, public utility commissions, water and sewer boards, park commissions, housing authorities, public health agencies, and many others.

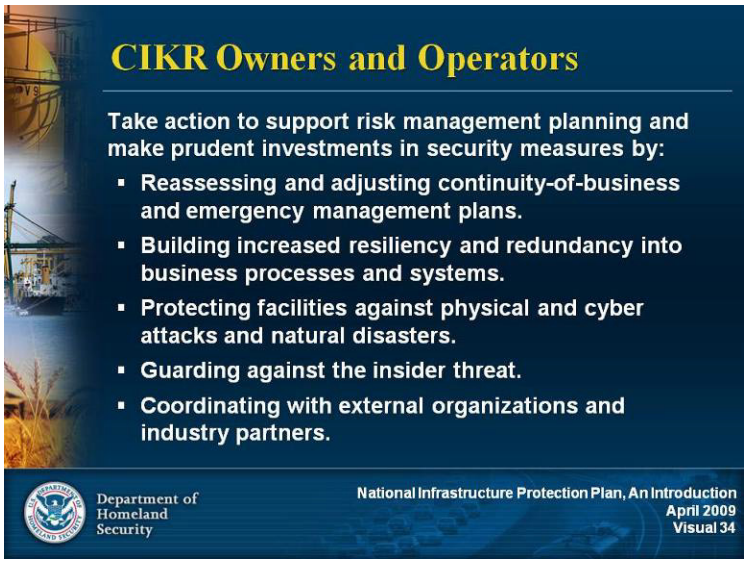
These entities may serve as SSAs within a State and contribute expertise, assist with regulatory authorities, or help to facilitate investment decisions related to CIKR protection efforts within a given jurisdiction or geographical region.

Best Practices (Commissions). Public utility commissions are responsible for electricity, gas, and telecommunications infrastructures and, in some cases, water, wastewater/sewage, and certain aspects of transportation. Working together, public utility commissions are able to address issues of mutual concern based on the interdependencies between the water, telecommunications, and energy infrastructures by:

- Creating networks among utility regulators and other Federal, State, local, and private sector entities to address cross-sector issues.
- Recommending strategies to facilitate information sharing.
- Recommending cost-effective solutions to cost-recovery issues associated with protecting key water, gas, communications, and energy infrastructures.
- Identifying and prioritizing issues, researching best practices, and disseminating information to Federal and State partners and affiliates.

Topic | **Roles**

Visual 34



Visual Description: CIKR Owners and Operators

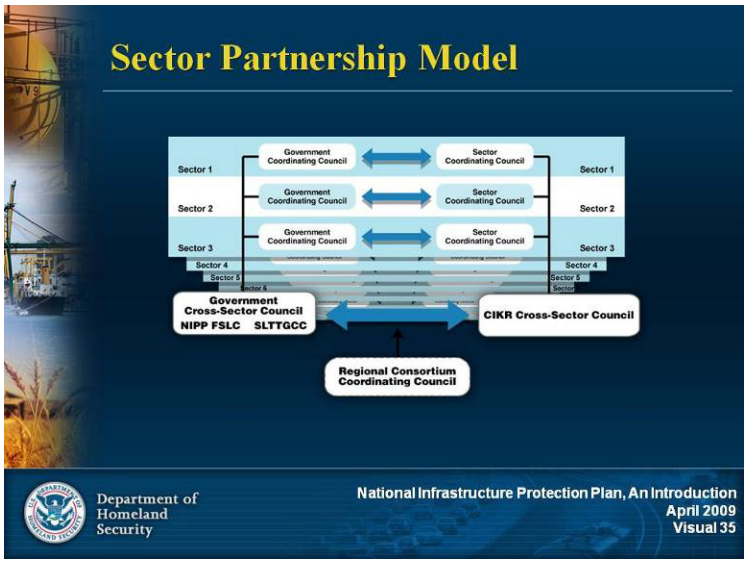
Instructor Notes

Owners and operators generally develop and implement the protective programs and resiliency strategies for the CIKR under their control. Owners take action to support risk management planning and investments as a necessary component of prudent business planning and operations. This includes:

- Reassessing and adjusting continuity-of-business and emergency management plans.
- Building increased resiliency and redundancy into business processes and systems.
- Protecting facilities against physical and cyber attacks and natural disasters.
- Guarding against the insider threat.
- Coordinating with external organizations to avoid or minimize the impacts on surrounding communities or other industry partners.

Topic | **Roles**

Visual 35



Visual Description: Sector Partnership Model

Instructor Notes

The NIPP relies on the sector partnership model as the primary organizational structure for coordinating CIKR efforts and activities. The sector partnership model encourages formation of Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs). SCCs and corresponding GCCs work in tandem to create a coordinated national framework for CIKR protection within and across sectors. This structure was developed based on guidance from private sector partners.

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 organizations and information-sharing network.

The sector partnership model provides:

- An integrated, networked, and consistent structure to foster coordination between private sector entities within the same industry to address common problems.
- A structure to foster coordination and collaboration between the private sector and the government.

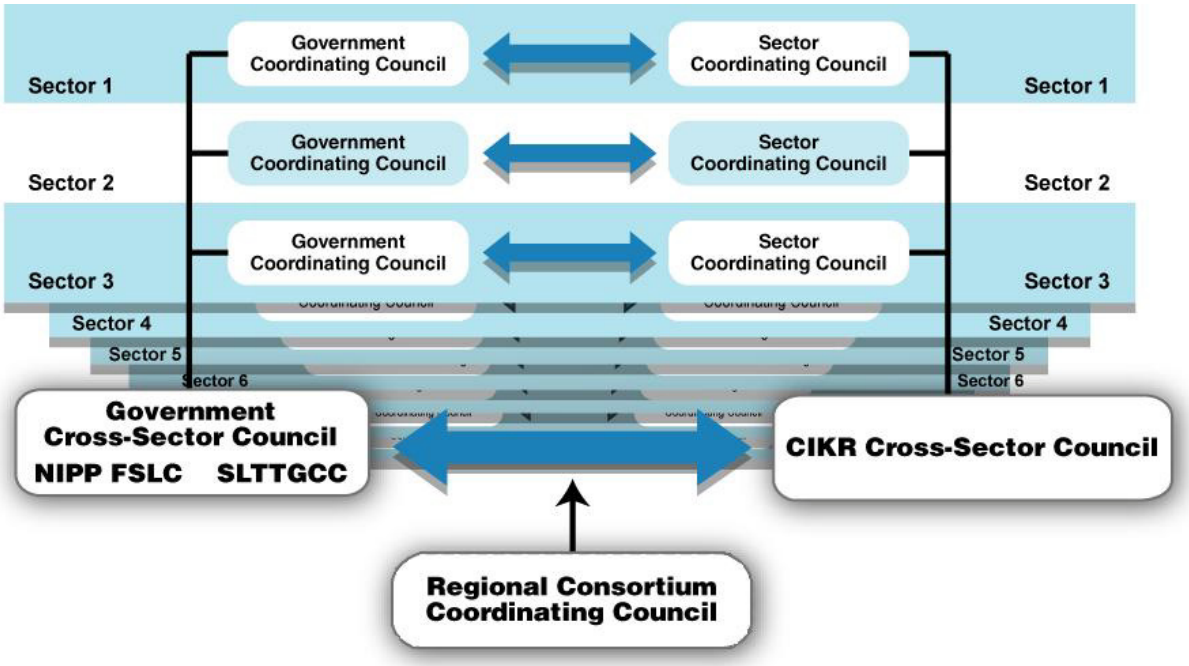
The scope and magnitude of this effort is **unprecedented.**

Encourage the participants to discuss the following issues:

- Why is this unprecedented?
- What are some of the obstacles that this type of a coordination structure helps to overcome?
- What are the benefits?

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

Topic | **Roles**



Caption: Graphic showing the sector partnership model, and the relationships between sectors and the Government Cross-Sector Council, CIKR Cross-Sector Council, and Regionally Based Councils.

Topic | **Roles**

Visual 36

Visual Description: Sector Coordinating Councils (SCCs)

Instructor Notes

The sector partnership model encourages CIKR owners and operators to create or identify a Sector Coordinating Council as the principal entity for coordinating with the government on a wide range of CIKR protection activities and issues.

Specific membership will vary by sector, reflecting the unique composition of each sector. However, membership should be representative of a broad base of owners, operators, associations, and other entities—large and small—within a sector.

Cross-sector issues and interdependencies are addressed among the SCCs through the CIKR Cross-Sector Council. The Partnership for Critical Infrastructure Security provides the representation of the leadership of each of the SCCs, with support from DHS's CIKR Executive Secretariat. The CIKR Cross-Sector Council provides senior-level, cross-sector strategic coordination through partnership with DHS and the SSAs.

Topic | **Roles**

Visual 37

Visual Description: Government Coordinating Councils (GCCs)

Instructor Notes

A Government Coordinating Council 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, and tribal) as appropriate to the operating landscape of each individual sector.

Cross-sector issues and interdependencies between the GCCs are addressed through the Government Cross-Sector Council and its two subcouncils.

Topic | **Roles**

Visual 38

Visual Description: CIKR Cross-Sector Council

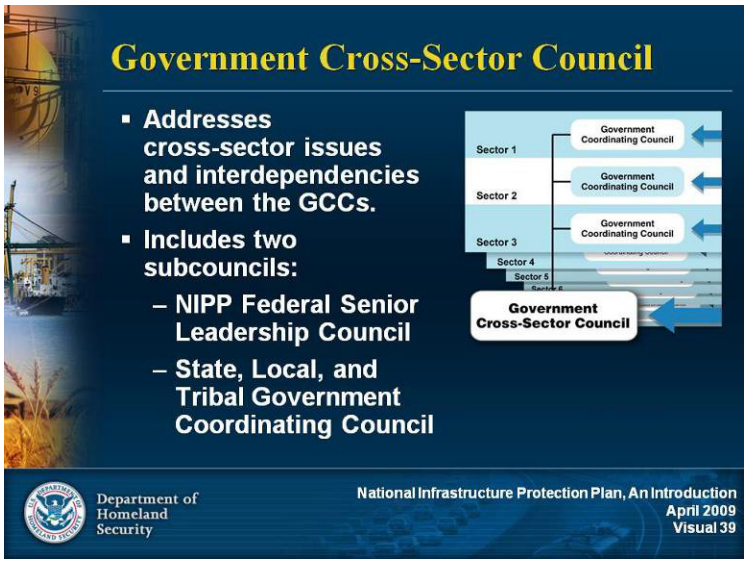
Instructor Notes

The CIKR Cross-Sector Council:

- Is known as the Partnership for Critical Infrastructure Security (PCIS).
- Provides senior-level, cross-sector strategic coordination through partnership with DHS and the SSAs.

Topic | **Roles**

Visual 39



Visual Description: Government Cross-Sector Council

Instructor Notes

The Government Cross-Sector Council addresses cross-sector issues and interdependencies between the GCCs, and includes the following subcouncils:

- **NIPP Federal Senior Leadership Council (FSLC).** The FSLC drives enhanced communications and coordination between and among Federal departments and agencies with a role in implementing the NIPP and HSPD-7.
- **State, Local, and Tribal Government Coordinating Council (SLTGCC).** The SLTGCC provides an organizational structure to coordinate across jurisdictions on State- and local-level CIKR protection, guidance, strategies, and programs.

Topic | **Roles**

Visual 40

Visual Description: Critical Infrastructure Partnership Advisory Council (CIPAC)

Instructor Notes

The CIPAC directly supports the NIPP sector partnerships by providing a legal framework for members of the SCCs and GCCs to engage in joint CIKR protection-related discussions. The CIPAC serves as a forum for government and private sector security partners to engage in a broad spectrum of activities, including planning, coordination, implementation, and operational issues.

The CIPAC membership consists of:

- Private sector CIKR owners and operators, or their representative trade or equivalent associations, from the respective sector's recognized SCC; and
- Representatives of Federal, State, local, and tribal government entities (including their representative trade or equivalent associations) that comprise the corresponding GCC for each sector.

Topic | **Roles**

Visual 41

Visual Description: Advisory Councils

Instructor Notes

Advisory Councils:

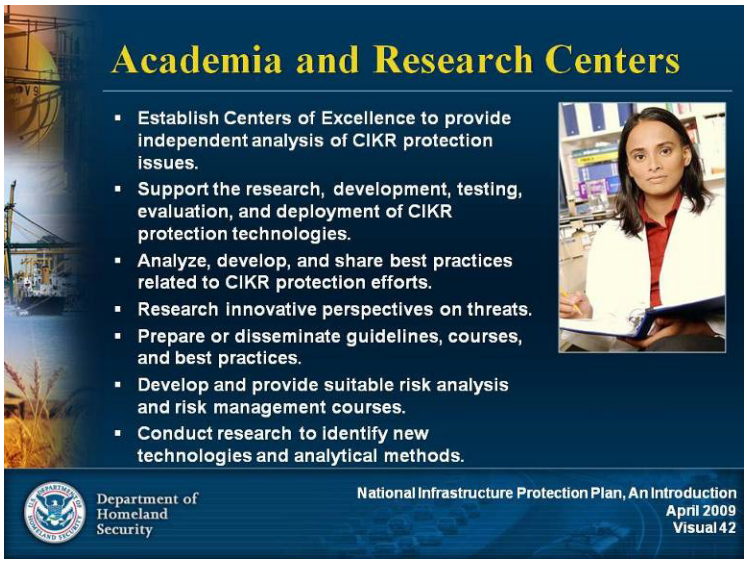
- Provide advice, recommendations, and expertise to the government regarding CIKR protection policy and activities.
- Help enhance public-private partnerships and information sharing.
- Offer an additional mechanism to engage with a pre-existing group of private sector leaders to obtain feedback on CIKR policy and programs, and to make suggestions to increase the efficiency and effectiveness of specific government programs.

Examples of CIKR protection-related advisory councils:

- **Homeland Security Advisory Council (HSAC):** The HSAC provides advice and recommendations to the Secretary of Homeland Security on relevant issues. The Council members, appointed by the Secretary of Homeland Security, include experts from State and local governments, public safety, security and first-responder communities, academia, and the private sector.
- **Private Sector Senior Advisory Committee (PVTSAC):** The Secretary of Homeland Security established the PVTSAC as a subcommittee of the HSAC to provide the HSAC with expert advice from leaders in the private sector.
- **National Infrastructure Advisory Council (NIAC):** The NIAC provides the President, through the Secretary of Homeland Security, with advice on the security of physical and cyber systems across all CIKR sectors. The Council comprises up to 30 members appointed by the President. Members are selected from the private sector, academia, and State and local governments.
- **National Security Telecommunications Advisory Committee (NSTAC):** The NSTAC provides industry-based advice and expertise to the President on issues and problems related to implementing National Security and Emergency Preparedness (NS/EP) communications policy. The NSTAC comprises up to 30 industry chief executives representing the major communications and network service providers and information technology, finance, and aerospace companies.

Topic Roles

Visual 42



Visual Description: Academia and Research Centers

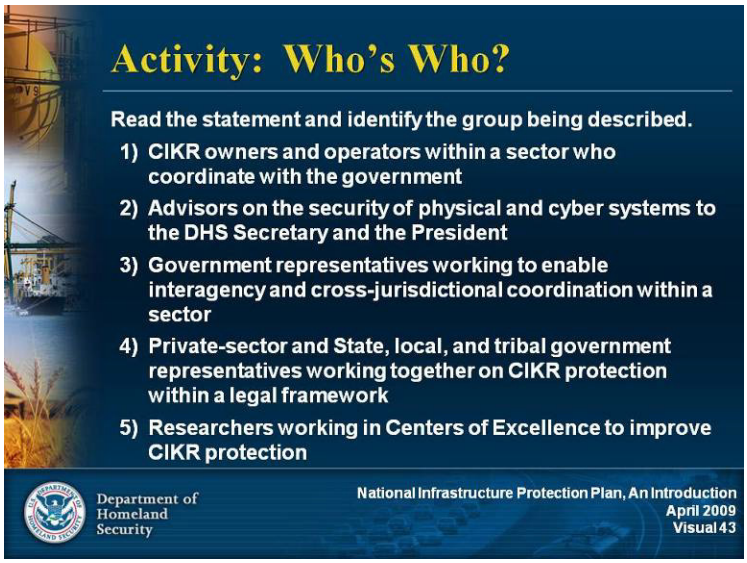
Instructor Notes

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

- Establishing Centers of Excellence (university-based partnerships or federally funded research and development (R&D) centers) to provide independent analysis of CIKR protection issues.
- Supporting the research, development, testing, evaluation, and deployment of CIKR protection technologies.
- Analyzing, developing, and sharing best practices related to CIKR prioritization and protection efforts.
- Researching and providing innovative thinking and perspective on threats and the behavioral aspects of terrorism.
- Preparing or disseminating guidelines, courses, and descriptions of best practices for physical security and cybersecurity.
- Developing and providing suitable all-hazards risk analysis and risk management courses for CIKR protection professionals.
- Conducting research to identify new technologies and analytical methods that can be applied by partners to support NIPP efforts.
- Establishing undergraduate and graduate curricula and degree programs.

Topic | **Activity**

Visual 43



Visual Description: Activity: Who's Who?

Instructor Notes

Ask the participants to read the statement and identify the group being described. Ask for volunteers to provide the answers.

1) CIKR owners and operators within a sector who coordinate with the government
2) Advisors on the security of physical and cyber systems to the DHS Secretary and the President
3) Government representatives working to enable interagency and cross-jurisdictional coordination within a sector
4) Private sector and State, local, and tribal government representatives working together on CIKR protection within a legal framework
5) Researchers working in Centers of Excellence to improve CIKR protection

If necessary, note the following answers:

1) Sector Coordinating Councils (SCCs)
2) National Infrastructure Advisory Council (NIAC)
3) Government Coordinating Councils (GCCs)
4) Critical Infrastructure Partnership Advisory Council (CIPAC)
5) Academia, research centers, and think tanks