3

Current Critical Infrastructure Protection

INTRODUCTION

Today, critical infrastructure (CI) protection is a top priority for officials in all levels of governments, including federal, state, local, and tribal structures. It is also a priority for both public owners and private owners and operators of CI. No matter who is involved, the goal is to protect our infrastructure from damage resulting from a man-made incident such as a terrorist attack, but also from a natural event such as a hurricane or earthquake. In either case, the object is to return a community to a normal (or close to normal) state of affairs as quickly as possible. Chapter 2 provided an early history of asset protection, and this chapter provides a description of the current policies for protecting the nation's infrastructure. These policies are in a continual state of flux as the government continues to improve CI protection in response to ever-changing threats.

OBAMA ADMINISTRATION

President Barack Obama, since taking office in 2009, has not made many changes to the infrastructure protection policies that were originally generated by Presidents Clinton and Bush. Instead, he has continued to build on existing structures. Early in his Presidency, in February 2009, President Obama asked for a review of the homeland security and counterterrorism

structures that were located within the White House. He also asked for an evaluation of the federal government's policies regarding cybercrime and cybersecurity. The results of the analysis were released in May 2009. Based on these reviews, the President merged the Homeland Security Council and the National Security Council into one agency, which he called the National Security Staff. The report also included a recommendation to appoint one person from the White House who would be responsible for overseeing federal policies regarding cybersecurity.

Strategic National Risk Assessment

In 2010, the Secretary of Homeland Security wrote the Strategic National Risk Assessment (SNRA). This was a classified assessment that formed the basis of Presidential Policy Directive 8 (PPD-8), which was announced by President Obama in 2011 (described in the section "Presidential Policy Directive-8"). The goal of the SNRA was to help identify the types of incidents that posed the greatest threat to the security of the nation. The committee that assisted the investigation included officials from the Director of National Intelligence and the Attorney General. An unclassified version of the report was released to the public in December 2011. Among other things, the report analyzed weaknesses in the nation's security and gave suggestions for how those could be addressed.

The committee drew from multiple sources, including historical records and experts from different disciplines. The Committee assessed the frequency and consequence of risks, to answer the question, *with what frequency is it estimated that an event will occur, and what are the consequences of the incident(s) if it does occur*? The Committee examined the threats and consequences associated with six categories of harm: (a) loss of life, (b) injuries and illnesses, (c) direct economic costs, (d) social displacement, (e) psychological distress, and (f) environmental impact.

The risks from possible threats and hazards that had the potential to have a significant impact on the nation's assets were discussed. The members identified risk factors, and then identified core capabilities and capability targets that would be described in the *National Preparedness Goal*. The committee members relied on a new approach to asset protection that relied on collaborative thinking about strategic needs for prevention, protection, mitigation, response, and recovery requirements. It also promoted the necessity for all levels of government to share a common understanding and awareness of threats and hazards so that they could prepare for, and respond to, events both independently and collaboratively. This was

critical because, as noted by the committee, preparation and response are often more effective when multiple responders from local, state, and federal agencies are involved. It was also recognized that the whole community should be involved.

Possible events that could affect the nation's security were grouped into three categories: (a) natural hazards; (b) technological/accidental hazards; and (c) adversarial, human-caused threats/hazards. The report also created six possible harms: (a) loss of life, (b) injuries and illnesses, (c) direct economic costs, (d) social displacement, (e) psychological distress, and (f) the environment. The SNRA Committee found that there were a wide range of threats and hazards that posed a significant risk to the nation, affirming the need for an all-hazards, capability-based approach to preparedness planning. Some of the key findings reported included the following:

1. Natural hazards, including hurricanes, earthquakes, tornados, wildfires, and floods, present a significant and varied risk across the country.
2. A virulent strain of pandemic influenza has the possibility of killing hundreds of thousands of Americans and affecting millions more, resulting in economic loss.
3. Technological and accidental hazards, such as dam failures or chemical substance spills or releases, could result in devastating fatalities and severe economic impacts. The likelihood of this happening may increase because of aging infrastructure.
4. Terrorist organizations or their affiliates may attempt to acquire, build, and use weapons of mass destruction (WMD). Conventional terrorist attacks, including those by "lone actors" employing explosives and armed attacks, present a continued risk.
5. Cyberattacks can have their own catastrophic consequences and can also cause other hazards, including power grid failures or financial system failures, which magnify the potential impact of cyber incidents.[1]

The SNRA Committee identified events that had the potential to pose the greatest risk to the security of the nation.[2] These are listed in Table 3.1. The Committee recognized that it was possible that many of the events they listed could potentially occur more than once every 10 years, meaning that the nation's preparedness would probably be tested at some point in the next 10 years. They also stressed that risks to CI are always changing, and the nation must always be prepared for new hazards.

Table 3.1 SNRA National Level Events

Threat/Hazard Group	Threat/Hazard Type	National Level Event Description
Natural	Animal disease outbreak	An unintentional introduction of the foot-and-mouth disease virus into the domestic livestock population in a US state
Earthquake	An earthquake occurs within the US resulting in direct economic losses greater than $100 million	
Flood	A flood occurs within the US resulting in direct economic losses greater than $100 million	
Human pandemic outbreak	A severe outbreak of pandemic influenza with a 25% gross clinical attack rate spreads across the US populace	
Hurricane	A tropical storm or hurricane impacts the US resulting in direct economic losses of greater than $100 million	
Space weather	The sun emits bursts of electromagnetic radiation and energetic particles causing utility outages and damage to infrastructure	
Tsunami	A tsunami with a wave of approximately 50 ft. impacts the Pacific Coast of the US	
Volcanic eruption	A volcano in the Pacific northwest erupts impacting the surrounding areas with lava flows and ash and areas east with smoke and ash	
Wildfire	A wildfire occurs within the US resulting in direct economic losses greater than $100 million	
Technological/ Accidental	Biological food contamination	Accidental conditions where introduction of a biological agent (e.g., *Salmonella*, *E. coli*, botulinum toxin) into the food supply results in 100 hospitalizations or greater and a multistate response
Chemical substance spill or release	Accidental conditions where a release of a large volume of a chemical acutely toxic to human beings (a toxic inhalation hazard, or TIH) from a chemical plant, storage facility, or transportation mode results in either one or more offsite fatalities, or one or more fatalities (either on- or offsite) with offsite evacuations/ shelter-in-place	
Dam failure	Accidental conditions where dam failure and inundation results in one fatality or more	

(*Continued*)

Table 3.1 SNRA National Level Events (*Continued*)

Threat/Hazard Group	Threat/Hazard Type	National Level Event Description
Radiological substance release	Accidental conditions where reactor core damage causes release of radiation	
Adversarial/ Human-caused	Aircraft as a weapon	A hostile nonstate actor(s) crashes a commercial or general aviation aircraft into a physical target within the US
Armed assault	A hostile nonstate actor(s) uses assault tactics to conduct strikes on vulnerable target(s) within the US resulting in at least one fatality or injury	
Biological terrorism attack (nonfood)	A hostile nonstate actor(s) acquires, weaponizes, and releases a biological agent against an outdoor, indoor, or water target, directed at a concentration of people within the US	
Chemical/ biological food contamination terrorism attack	A hostile nonstate actor(s) acquires, weaponizes, and disperses a biological or chemical agent into food supplies within the US supply chain	
Chemical terrorism attack (nonfood)	A hostile nonstate actor(s) acquires, weaponizes, and releases a chemical agent against an outdoor, indoor, or water target, directed at a concentration of people using an aerosol, ingestion, or dermal route of exposure	
Cyberattack against data	A cyberattack which seriously compromises the integrity or availability of data (the information contained in a computer system) or data processes resulting in economic losses of $1 billion or greater	
Cyberattack against physical infrastructure	An incident in which a cyberattack is used as a vector to achieve effects which are beyond the computer (i.e., kinetic or other effects), resulting in one fatality or greater or economic losses of $100 million or greater	
Explosives terrorism attack	A hostile nonstate actor(s) deploys a man-portable improvised explosive device (IED), vehicle-borne IED, or vessel IED in the US against a concentration of people, and/or structures such as critical commercial or government facilities, transportation targets, or critical infrastructure (CI) sites, etc., resulting in at least one fatality or injury	

Source: Department of Homeland Security. December 2011. *Strategic National Risk Assessment* (dhs.gov).

Executive Order 13563

On January 18, 2011, President Obama issued Executive Order 13563, which was entitled "Improving Regulation and Regulatory Review." In this document, Obama reaffirmed the mandates set forth in Executive Order 12866, known as "Regulatory Planning and Review." In the new Executive Order, Obama directed all federal agencies to develop a preliminary plan to review their regulations to determine whether any of the existing rules should be updated or altered in any way to make the agency's regulatory program more effective.

One example of this was the DHS Preliminary Plan, which became public on May 26, 2011. A primary focus of their plan was to include members of the public as part of the review process. They also sought to include members of the public in the development of the plan and then the implementation of it.[3]

Presidential Policy Directive-8

On March 30, 2011, President Obama signed the Presidential Policy Directive-8 (PPD-8), entitled *National Preparedness*. This document replaced Homeland Security Presidential Directive-8 (HSPD-8) that was signed by President George W. Bush in 2003. In the new document, Obama developed a way to further strengthen the nation's security and resilience by making the nation better prepared for events. He concentrated on an all-hazards approach to security that included planning for possible terrorist acts, including cyberattacks, technological events, and also natural disasters. Additionally, the president recognized that national preparedness and security must involve all people who have a personal stake in CI or security, including those in government, the private sector, and individual citizens. The document requires that everyone be involved in the process for protecting assets instead of just government officials, which was primarily what was done in the past.

Five mission areas were identified in PPD-8. They are Prevent, Protect, Mitigate, Respond, and Recovery, described as follows:

1. Prevent: This was recognized as the most important of the mission areas. While people cannot prevent natural weather-related events, it is possible to prevent man-made events. This includes taking any actions necessary to avoid, prevent, or stop a threatened or actual act of terrorism, or preventing imminent threats of any kind. Prevention-related activities may include: increased

inspections; more surveillance and security operations; efforts geared toward increased public health (e.g., immunizations); surveillance and testing of agricultural products; law enforcement operations aimed at deterring or disrupting illegal activity.
2. Protect: This involves taking actions necessary to secure the homeland against acts of terrorism and man-made or natural disasters. Keywords in this area are "defense," "protection," "protect," "security," and any kind to include "cybersecurity." This refers to efforts for protecting all citizens, residents, visitors, as well as physical assets against threats, and hazards in a way that allows people to continue their way of life.
3. Mitigate: This refers to actions geared toward reducing the loss of life and property that could occur after an event by lessening the impact of disasters. Keywords are "risk reduction," "improve resilience," and "reduce future risk."
4. Respond: In this category, the focus is on ensuring that people have the services needed after an event to save lives, protect property and the environment, and meet basic human needs. This includes responding quickly and ensuring that people have services they need to survive. To do that, it is essential that policies are created that coordinate federal, state, and local activities.
5. Recovery: This stage focuses on the providing services needed to assist affected communities to return to a "normal" state as quickly as possible. Keywords are "rebuilding," "restoring," "promoting," "interim," and "long term."[4] Efforts here focus on the timely restoration of services, strengthening and rebuilding of infrastructure, housing, and health facilities, as well as social, cultural, and historic elements of a community.[5]

In addition, there are also six elements noted in PPD-8: *National Preparedness Goal*; *National Preparedness System*; *National Preparedness Report*; *National Planning Frameworks*; *Federal Interagency Operational Plans*; and *Build and Sustain Preparedness*.

National Preparedness Goal

PPD-8 required the Secretary of Homeland security to create a new *National Preparedness Goal*.[6] According to Obama, "The National Preparedness Goal shall be informed by the risk of specific threats and vulnerabilities—taking into account regional variations—and include concrete, measurable, and prioritized objects to mitigate that risk."[7]

The goal identifies and defines core capabilities that, according to the president, the country needs in order to achieve preparedness and, in the end, better national security. When met, the core capabilities will help the country to be prepared for all types of incidents that could pose a risk to the nation's security. These core capabilities are essential for officials to implement the five mission areas as described earlier. The goal defines success as "A secure and resilient Nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk."[8]

A fundamental concept throughout the document is the emphasis on the whole community approach. This means that all interested groups and organizations need to work together in a variety of ways and make the best use of resources to be fully prepared for an event (see Note 4, pp. 1–13). In December 2011, Federal Emergency Management Agency (FEMA) relea sed a report entitled *A Whole Community Approach to Emergency Management: Principles, Themes and Pathways for Action*.[9] In this document, officials describe the idea of whole community approach. It means that all members of a community, including emergency management practitioners, community leaders, organizations, government officials, private business owners and operators, and citizens can each help to assess the needs of their own community and decide the best method to organize and strengthen their assets, capacities, and interests. They will decide the best ways to prepare to potential threats and hazards. This concept is described in Table 3.2.

Table 3.2 Key Principles of the Whole Community Approach

1. Understand and meet the actual needs of the whole community: community engagement can lead to a deeper understanding of the unique and diverse needs of a population, including its demographics, values, norms, community structures, networks, and relationships. The more we know about our communities, the better we can understand their real-life safety, sustaining needs, and their motivations to participate in emergency management-related activities prior to an event.
2. Engage and empower all parts of the community: engaging the whole community and empowering local action will better position stakeholders to plan for and meet the actual needs of a community and strengthen the local capacity to deal with the consequences of all threats and hazards. This requires all members of the community to be part of the emergency management team, which should include diverse community members, social and community service groups and institutions, faith-based and disability groups, academia, professional associations, and the private and

(*Continued*)

Table 3.2 (*Continued*) Key Principles of the Whole Community Approach

nonprofit sectors, while including government agencies who may not traditionally have been directly involved in emergency management. When the community is engaged in an authentic dialogue, it becomes empowered to identify its needs and the existing resources that may be used to address them.
3. Strengthen what works well in communities on a daily basis: a *Whole Community approach* to building community resilience requires finding ways to support and strengthen the institutions, assets, and networks that already work well in communities to address issues that are important to community members on a daily basis. This includes structures and relationships that are present in the daily lives of individuals, families, businesses, and organizations before an incident occurs.

Source: Federal Emergency Management Agency. December 2011. A Whole Community Approach to Emergency Management. FDOC 104-008-1, http://www.fema.gov/media-library-data.

National Preparedness System

The National Preparedness System refers to a document published in November 2011 that outlines an approach, resources, and tools needed to assist communities and the nation in meeting the National Preparedness Goal. It includes national planning frameworks that cover the five areas of prevention, protection, mitigation, response, and recovery, as mentioned earlier. The frameworks each use a common terminology and approach, and are each built around the all-hazards approach to preparedness. In addition, the system is also built on an "All-of-Nation" approach to preparedness. The system has six parts: (a) identifying and assessing risk; (b) estimating capability requirements; (c) building and sustaining capabilities; (d) planning to deliver capabilities; (e) validating capabilities; (f) reviewing and updating (see Note 4, pp. 1–13).

National Preparedness Report

Under the PPD-8, the Secretary of Homeland Security must submit a National Preparedness Report to the President each year. This report is to include a summary of the progress that has been made toward achieving the National Preparedness Goal. The Secretary is also required to identify any gaps in activities. The report could be used by the president when establishing the annual budget so that funds could be allocated to support existing activities or create new activities to fill the gaps (see Note 4, pp. 1–13).

National Planning Frameworks

There are five frameworks that focus on the mission areas of PPD-8 (Prevention, Protection, Mitigation, Response and Recovery). The frameworks demonstrate how different groups and agencies will cooperate to meet the needs of individuals, families, communities, and states in their efforts to prevent, protect, mitigate, respond to, and recover from any disaster or event (see Note 4, pp. 1–13).

The frameworks were created in a way that they are scalable and could be adapted to each individual community or event. The frameworks only establish the overall theme or strategy (coordinating structure) for communities, which must then build and deliver the core capabilities identified in the National Preparedness Goal. It was stressed that there is a need for a common terminology that will be used across all of the frameworks as a way to ensure interoperability across all mission areas. The frameworks address the roles of individuals, nonprofit entities, government agencies, nongovernmental organizations (NGOs), the private sector, and communities in planning for response to events. Most importantly, the frameworks contain detailed information on the 31 core capabilities, which help to define desired outcomes, set capability targets, and specify appropriate resources.

Federal Interagency Operational Plans

These plans describe the federal government's strategies to deliver the core capabilities outlined in the five frameworks described earlier. These plans help to define how federal policies and officials can provide support to state and local officials as they establish plans for responding to an event. The federal plans will also describe essential tasks and responsibilities and specific provisions for integrating resources and personnel with other governments (see Note 4, pp. 1–14).

Build and Sustain Preparedness

This element stresses that the effort to build and maintain the country's preparedness is ongoing and will constantly build on existing activities (see Note 4, pp. 1–14).

This element has four key sections, which are as follows:

1. A comprehensive campaign, including public outreach and community-based and private sector programs
2. Federal preparedness efforts
3. Grants, technical assistance, and other federal preparedness support
4. Research and development

Executive Order 13636

On February 12, 2013, President Obama issued Executive Order 13636, *Improving Critical Infrastructure: Cybersecurity*. In this document, the president stressed that the nation's security depends on a reliable and functioning CI and a secure cyber environment. He also stressed that the best way to achieve a safe environment is with better communication and cooperation with the owners and operators of CI. Clearly, increased communication could lead to more efforts to collaborate on, develop, and implement risk-based approaches to cybersecurity. For these reasons, Obama asked the federal government to coordinate their activities with the owners and operators of CI and improve information sharing between the groups. As another way to improve information sharing, Obama asked the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence to develop unclassified reports on any cyberthreats that are reported, and to share those reports with the targeted group.

In another part of the executive order, Obama sought to develop a cybersecurity framework for CI, to improve the nation's cybersecurity. This framework would establish standards, methodologies, procedures, and processes that the owners of CI could use to reduce their cybersecurity risks. The new plan, when done, would be a cost-efficient approach to helping owners and operators identify, assess, and manage cyber risks. The plan will help owners and operators identify potential vulnerabilities, then provide innovative suggestions for addressing those risks. The process of creating the framework would be overseen by the Director of the National Institute of Standards and Technology (NIST), but other interested people would be allowed to participate. This would include sector coordinating councils, owners and operators of critical assets, Sector-Specific Agencies (SSAs), regulatory agencies, universities, and other relevant groups. The framework would be the basis for the Voluntary CI Cybersecurity Program.

The framework was released in February 2014. Upon its release, all owners or operators of CI were encouraged to use the framework to improve the security of their networks. Any agencies that had the responsibility of regulating the security of CI were asked to review their policies to determine if they were sufficient, and if not, they were asked to consider adopting the recommended ones, or at least modifying what they had to align more with the standards found in the framework. The Secretary of Homeland Security was also asked to create incentives for participating in the voluntary program.

The Enhanced Cybersecurity Services program was expanded through Obama's executive order. This program allows classified information on cybersecurity threats and other technical information to be shared with infrastructure network service providers. Obama asked government agencies to expand the program to all CI sectors so that more information about threats and other technical information would be shared with a bigger audience more quickly. In order for this to work, Obama asked to change the way security clearances to those employed by infrastructure owners and operators were granted, making the process quicker.

At the same time, the president wanted to ensure that privacy and civil liberties of all individuals were protected. He asked that the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the DHS oversee the programs and recommend ways to ensure that citizens' rights were protected.

Executive Order 13691

In February 2015, Obama issued Executive Order 13691, called *Promoting Private Sector Cybersecurity Information Sharing*. In this document, he addressed the importance of sharing information pertaining to cybersecurity. Obama gave the Secretary of DHS the responsibility of establishing Information Sharing and Analysis Organizations (ISAOs), which are very much like the Information Sharing and Analysis Centers (ISACs) in PDD-63. There would also be an ISAO Standards Organization that would work with all of the CI stakeholders to develop voluntary standards and guidelines for establishing and operating ISAOs. In the Executive Order, Obama also designated the National Cybersecurity and Communications Integration Center (NCCIC) as a CI protection program, allowing it to receive and transmit cybersecurity information between the federal government and the ISAOs as protected CI information.

Presidential Policy Directive-21

In February 2013, President Obama announced Presidential Policy Directive-21 (PPD-21), which had the title *Critical Infrastructure Security and Resilience*. This new plan superseded Homeland Security Presidential Directive (HSPD-7) from the Bush administration. PPD-21 reflected the increased interest in resilience and the all-hazard approach that has evolved in CI protection policy over the last few years. The purpose of the directive was to establish a national policy to strengthen and maintain a

secure CI that is also resilient to attacks. This is important for the continuity of national essential functions. Both physical and cyber infrastructure was included.

In PPD-21, cooperation was stressed. Companies were asked to cooperate not only with the government but sometimes with competing industries in efforts to increase security. As noted by Obama, CI protection must be a shared responsibility between federal, state, local, tribal, and territorial entities, along with public and private owners and operators of the assets. He also noted the importance of working with international partners to strengthen infrastructure that was physically located outside the US.

The number of sectors and how they are organized were changed in PPD-21 (see Table 3.3). In the 2006 National Infrastructure Protection Plan (NIPP), there were 17 CI sectors established, as outlined in HSPD-7. But since PPD-21 revoked HSPD-7, the 18 sectors were reorganized into 16 CI sectors.

PPD-21 identifies the energy and communications sectors as uniquely critical and deserving of extra attention (see Note 4, pp. 1–7). National Monuments and Icons was designated as a subsector of Government

Table 3.3 16 Critical Infrastructure and Key Resources Sectors

1. Chemical Sector: Department of Homeland Security (DHS) is the Sector-Specific Agency (SSA)
2. Commercial Facilities Sector: DHS is the SSA
3. Communications Sector
4. Critical Manufacturing: DHS
5. Dams: DHS
6. Defense Industrial Base Sector
7. Emergency Services Sector
8. Energy Sector
9. Financial Services Sector
10. Food and Agriculture Sector Department of Agriculture and Department of Health and Human Services are co-SSAs
11. Government Facilities Sector: DHS and General Services Administration (GSA)
12. Healthcare and Public Health Sector
13. Information Technology Sector
14. Nuclear Reactors, Materials and Waste Sector; DHS
15. Transportation Systems Sector: DHS and Department of Transportation
16. Water and Wastewater Systems Sector: Environmental Protection Agency (EPA)

Facilities; Postal and Shipping was designated as a subsector of Transportation; Banking and Finance was renamed Financial Services; and Drinking Water and Water Treatment was renamed Water and Waste Water Systems. In March 2008, DHS announced the creation of an additional sector, Critical Manufacturing. The sector encompasses groups from the primary metal, machinery, electrical equipment, and transportation equipment manufacturing industries. PPD-21 also gave the energy and communications sectors a higher profile, because of the Administration's assessment of their importance to the operations of the other infrastructures.

PPD-21 also called for other federal departments and agencies to play a key role in CI security and resilience activities through their appointment as SSA. An SSA is a federal department or agency that is responsible for, among other things, security, and resilience programs and related activities of designated sectors. Each sector was assigned a SSA (see Table 3.3). For example, DHS is the SSA for the commercial facilities and dams sectors, and the Department of Energy (DOE) and the Environmental Protection Agency (EPA) are the SSAs for the energy and water sectors, respectively. DHS also shares SSA responsibilities with the Department of Transportation (DOT) for the transportation sector, and the General Services Administration (GSA) for the government facilities sector.[10] The lead agency assignments are noted in Table 3.4.

1. While energy shows as one sector, it is actually represented by two separate sectors: electric power (except for nuclear power facilities); and the production, refining, and some distribution of oil and gas. The DOE is the lead agency for both. However, the Department of Homeland Security (DHS) (through the Transportation Security Administration) is the lead agency for the distribution of oil and gas via pipelines. Nuclear power is considered to be its own sector.
2. Transportation includes all modes of transportation: rail, mass transit (rail and bus), air, maritime, highways, pipelines, and so forth. The Transportation Security Administration (part of the DHS), in collaboration with the DOT, is the lead agency for all but the maritime subsector, which has the Coast Guard (also within the DHS), as its lead agency.

President Obama asked for an evaluation of the existing public–private partnership model to determine if it could be improved. To do this, he sought to collect baseline data and existing system requirements that would be the starting point for a more efficient exchange of information.

Table 3.4 Current Lead Agency Assignments

Department/Agency	Sector/Subsector
Agriculture	Agriculture, food
Agriculture	Meat/poultry
Health and Human Services	All other
Treasury	Financial services (Formerly Banking and Finance)
EPA	Water and wastewater systems (formerly drinking water and water treatment systems)
Health and Human Services	Public Health and Healthcare
Defense	Defense Industrial Base
Energy	Energy
Homeland Security	Transportation systems (now includes postal and shipping)
Homeland Security	Information technology
Homeland Security	Commercial nuclear reactors, materials, and waste
Homeland Security	Chemical
Homeland Security	Emergency services
Homeland Security	Dams
Homeland Security	Commercial facilities
Homeland Security	Government facilities (now includes national monuments and icons)
Homeland Security	Critical manufacturing

After this was established, a new plan would be developed, called the Research and Development Plan for CI, which would be a working document that would be updated every 4 years.

Throughout PPD-21, the president outlined the roles and responsibilities of different groups as the following:

1. The Secretary of Homeland Security "shall provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure." This person should evaluate national capabilities and challenges to protecting assets, analyze threats and vulnerabilities, and develop a national plan. The DHS was also asked to identify and prioritize infrastructure, maintain

centers that provide situational awareness (i.e., emerging trends, imminent threats, or status of incidents), provide information and analysis on information, assess vulnerabilities, and coordinate federal government responses to significant incidents.
2. SSAs were asked to provide sector specific information and expertise about their specific sector, and then coordinate their activities and plans with DHS and other agencies. They can also provide technical assistance if needed either to mitigate incidents or respond to incidents.
3. The Department of State was asked to work with representatives from other countries to strengthen the security and resilience of any CI located outside of the US.
4. The Department of Justice (the FBI) was identified as the organization that would lead counterterrorism and counterintelligence investigations to disrupt and reduce foreign intelligence and actual or attempted attacks on the nation's infrastructure.
5. Department of Interior should identify and coordinate security and resilience efforts for all monuments and icons.
6. The Department of Commerce was given the responsibility to engage the private sector, research, and academic organizations as a way to improve security of cyber-based systems, and help to develop new ways to protect CI.
7. The Intelligence Community should provide intelligence assessments regarding possible threats.
8. The GSA was given the task of providing contracts for CI systems that include audit rights for the security and resilience of assets.
9. The Nuclear Regulatory Commission should oversee the protection of commercial nuclear power reactors, as well as the transportation of nuclear waste.
10. The Federal Communications Commission was asked to identify vulnerabilities in the Communications Sector and work to address those.

In addition to all of this, there were three strategic imperatives outlined by President Obama in the Directive. These were as follows[11]:

1. To refine and clarify functional relationships across the federal government as a way to advance CI security and resilience. If needed, relationships among stakeholders should be defined or even redefined. The functions of federal agencies need to be clarified to reflect an increase in knowledge and changes in threats. To

do this, President Obama asked for two national centers operated by DHS that would work to enhance CI protection. One would focus on physical infrastructure and the other on cyber protection.
2. Enable efficient exchange of information between all levels of government as well as with all owners and operators of CI. There is a need for more information sharing within the government and with the private sector.
3. Implement an analysis of incidents or threats to inform planning and operational decisions regarding CI protection. This should include operational and strategic analysis.

NIPP 2006

In PPD-21, President Obama required that the NIPP be updated and revised. The NIPP had originally been published in 2006, but the administration believed it was time to update that plan. The updated plan was to include a focus on the how the sectors rely on the energy and communications infrastructure and ways to mitigate the associated risks. Clearly, there had been significant changes in the risk, policy, and operating environments surrounding the country's CI since the NIPP was first published.

The 2006 version of the NIPP outlined an integrated national plan for managing risk for the country's CI. The process included identifying assets and threats, then conducting threat assessments in which vulnerabilities were analyzed in light of consequences and risk mitigation activities. Those activities would be prioritized based on cost-effectiveness. The 2006 NIPP also called for implementation plans for these risk reduction activities.

Each lead agency was asked to work in collaboration with other agencies in its sector to write a Sector-Specific plan. When the plans were completed, DHS was to integrate the individual Sector-Specific Plans into a national plan. This could then be used to identify the assets that, if damaged, could pose a significant risk to the entire nation. Any risk reduction plans that required federal assistance would also be identified. The sector officials were asked to review the plans every 3 years and reissue revised plans if needed. This would help ensure that the plans would remain current and relevant to all security partners.

Only seven plans were made public, and the others were given the designation "For Official Use Only." The Government Accountability

Office (GAO) reviewed nine of the plans and found that all complied with the NIPP process. However, some of the plans were more complete than others and provided more analysis than others. There were significant differences in the amount of detail provided and the general thoroughness of the reports. Moreover, while all of the plans provided detail about the threat analyses conducted by the sector, eight of the plans described no incentives that the sector could use to encourage owners and operators to carry out voluntary risk assessments, as required by the NIPP. These incentives were needed since many of the companies in the sectors were privately owned, they were not regulated by the government. Instead, the government was forced to rely on voluntary compliance with the NIPP.

The GAO finished their report by making two key recommendations to DHS. First, they recommended that the DHS provide better definitions of CI information needs; and second, that there be a better explanation of how this information could be used to attract more users.

NIPP 2013

After a brief revision in 2009, the NIPP was again revised in 2013 after President Obama, in PPD-21, called for officials to update the document. He requested the update based on a belief that there had been significant changes in the CI risk, policy, and operating environments, as well as our general knowledge about CI protection. In essence, government officials and others were to complete a "gap analysis" to fix any gaps that may exist in asset protection. The 2013 National Plan builds upon previous NIPPs and emphasizes goals of CI security and resilience. The ultimate goals were to: (a) identify, deter, detect, disrupt, and prepare for threats and hazards to the nation's CI; (b) reduce vulnerabilities of critical assets, systems, and networks; and (c) mitigate the potential consequences of incidents or adverse events that do occur to infrastructure (see Note 4, p. 1–9).

The revised NIPP was developed through a collaborative process that included stakeholders from the 16 CI sectors, all 50 states, and from all levels of government and industry. The Committee members worked to identify priorities and articulate goals that would help to mitigate risk to infrastructure and help be resilient in the case of an attack. As published, the following are the vision, mission, and goals:

Vision: A nation in which physical and cyber infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened.

Mission: Strengthen the security and resilience of the nation's CI by managing physical and cyber risks through the collaborative and integrated efforts of the CI community.

Goals:

1. Assess and analyze threats to, vulnerabilities of, and consequences to CI to inform risk management activities.
2. Secure CI against human, physical, and cyberthreats through sustainable efforts to reduce risk, while accounting for the costs and benefits of security investments.
3. Enhance CI resilience by minimizing the adverse consequences of incidents through advance planning and mitigation efforts, and employing effective responses to save lives and ensure the rapid recovery of essential services.
4. Share actionable and relevant info across the infrastructure community to build awareness and enable risk-informed decision making.
5. Promote learning and adaptation during and after exercises and incidents.[12]

The 2013 NIPP, entitled *Partnering for Critical Infrastructure and Resilience*, is largely the same as the two earlier versions, but with more integration of resiliency and the all-hazard approach. However, the basic partnership model and the risk management framework were maintained. The revised NIPP stresses the importance of developing partnerships between national, regional, state, and local government and owners and operators. It was made clear that coordination with infrastructure stakeholders is necessary to protect the public's safety and ensure national security.

The revised NIPP made it clear that managing the risks from threats and hazards requires an integrated approach as a way to identify, deter, detect, disrupt, and prepare for threats and hazards to the nation's CI; reduce vulnerabilities of critical assets, systems, and networks; and then mitigate the potential consequences to CI of incidents or adverse events that do occur.[13]

The new report recognized that the country's well-being relies on security and resiliency of CI, so the primary goal of any program must be the efforts to protect CI. To do that, the NIPP establishes a procedure to define what assets are considered to be national CI and how to protect them. International collaboration is also part of asset protection efforts. The new report also gives attention to cybersecurity (see Note 13).

Cooperation with the all partners was stressed, particularly with private sector owners and operators of CI, alongside of federal, state, local, tribal and territorial governments, regional entities, NGOs, and academia (see Note 4, pp. 1–8). The document stressed that these groups should work together to manage risks and achieve better security. Because everyone is involved in the process, many perspectives will be included, resulting in better information sharing (see Note 13, pp. 1–8). To increase cooperation, many groups were included in the process. These include sector coordinating councils, government coordinating councils, and cross-sector councils.

Better communication was also needed by federal agencies to help to prevent the "silo effect" whereby an agency carries out a program but does not communicate that with other agencies. This can lead to wasted resources, but also inefficiencies and gaps in services.

The 2013 NIPP highlights seven core tenets and twelve action items to guide the national effort over the next 4 years. These are described in Table 3.5.

The NIPP uses a five-step risk management framework that is applicable to the general threat environment as well as to specific threats or incidents. The five steps can be applied to physical (tangible property), cyber (electronic communications and information), and human security (knowledge of people susceptible to attack). The five steps are as follows[14]:

1. Set goals and objectives: Define specific outcomes, conditions, end points, or performance targets that collectively constitute an effective risk management posture.
2. Identify infrastructure and assets: Build, manage, refine, and improve a comprehensive inventory of the assets, systems, and networks that make up the nation's CI.
3. Assess and analyze risks: Evaluate the risk, taking into consideration the potential direct and indirect consequences of all-hazards threats and known vulnerabilities. These risks can be compared in order to develop a more complete view of asset, system, and/or network risks and associated mission continuity, where applicable. It is also possible to establish priorities based on risk attached to an asset.
4. Implement protective programs and resilience strategies (implement risk management activities): Select appropriate actions or programs to reduce or manage the risk identified, and identify and provide the resources needed to address priorities.

Table 3.5 2013 NIPP: Guiding Tenets and Call to Action

Tenets	Call to Action
Risk should be identified and managed in a coordinated and comprehensive way across the critical infrastructure (CI) community	Build upon partnership efforts
Understanding and addressing cross-sector (inter)dependencies is essential	Set national focus through jointly developed priorities
Gaining knowledge of risks and interdependences requires information sharing	Determine collective actions through joint planning efforts
The partnership approach recognizes the unique perspectives and comparative advantages of the diverse CI community	Empower local and regional partnerships to build capacity
Regional and state, local, tribal and territorial (SLTT) partnerships are crucial to improve security and resilience.	Leverage incentives to advance security and resiliency
Infrastructure critical to US transcends national boundaries, requiring cross-border cooperation	Innovate in managing risk
Security and resilience should be considered during the design of assets, systems, and networks	Enable risk-informed decision making through enhanced situational awareness
	Analyze infrastructure (inter) dependencies and cascading effects
	Promote recovery following incidents
	Strengthen development and delivery of technical assistance, training and education
	Improve security and resilience by research and Development
	Focus on outcomes
	Evaluate progress toward achieving goals
	Learn and adapt

5. Measure effectiveness: Use metrics and other evaluation procedures at the appropriate national, state, local, regional, and sector levels to measure progress and to assess the effectiveness of the CI Protection programs. In this case, those involved are able to track their progress and use the data as a baseline for comparison and continuous improvement through program implementation.

CONCLUSION

Since becoming president, Barack Obama has, for the most part, slowly expanded the policies, organizations, and programs that govern the protection of the nation's CI and assets. He has focused on expanding the involvement of all interested parties in the planning process and improving communication among all involved. President Obama has also focused on the all-hazards approach to protecting CI, and has expanded protection efforts into cybersecurity policies.

REVIEW QUESTIONS

1. How has President Obama addressed CI protection?
2. What was the intent of PPD-8?
3. Describe the impact of PPD-21.
4. What are the key principles of the whole community approach?
5. What are the changes made in Executive Order 13691?
6. What are some differences between the 2006 NIPP and the 2013 version?

NOTES

1. DHS, FEMA. September 2010. *CIKR Awareness AWR-213, Participant Guide*. Washington, DC: US DHS, pp. 1–19.
2. Department of Homeland Security. December 2011. *Strategic National Risk Assessment* (dhs.gov).
3. US DHS. July 27, 2015. *DHS Implementation of Executive Order 13563*. Retrieved from: http://www.dhs.gov/dhs-implementation-executive-order-13563.
4. DHS, FEMA. September 2014. *Critical Asset Risk Management, Participant Guide*, pp. 1–17.
5. US DHS. 2005. *National Response Plan Brochure*. Washington, DC: US DHS.

6. US DHS, FEMA. 2012. *Learn About Presidential Policy Directive 8*; also DHS, FEMA. September 2014. *Critical Asset Risk Management, Participant Guide*, pp. 1–12.
7. Obama, B. 2011. Presidential Policy Directive 8.
8. US DHS. 2011. *National Preparedness Goal*, p. 1.
9. Federal Emergency Management Agency. December 2011. A Whole Community Approach to Emergency Management. FDOC 104-008-1. Retrieved from: http://www.fema.gov/media-library-data.
10. US Department of Homeland Security, and US Department of Justice, Global Justice Information Sharing Initiative. December 2008. *Critical Infrastructure and Key Resources, Protection Capabilities for Fusion Centers*. Retrieved from: https://it.ojp.gov/documents/d/CIKR%20protection%20capabilities%20for%20fusion%20centers%20s.pdf.
11. The White House: Office of the Press Secretary. 2013. *Presidential Policy Directive—Critical Infrastructure Security and Resilience*.
12. US DHS. 2013. *National Infrastructure Protection Plan*, p. 5; DHS, FEMA. September 2014. *Critical Asset Risk Management, Participant Guide*, pp. 1–11.
13. US DHS. 2013. *National Infrastructure Protection Plan*.
14. DHS, FEMA. September 2010. *CIKR Awareness AWR-213, Participant Guide*, pp. 3–8.