Chapter 24

National Protection & Programs Directorate

Learning Outcomes

Careful study of this chapter will help a student do the following:

- Explain the mission of the organization.
- Describe some key components of the organization.
- Discuss some of the work of the organization.

"Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure – including assets, networks, and systems – that are vital to public confidence and the Nation's safety, prosperity, and well-being. "

- 2013 Presidential Policy Directive No. 21

Introduction

If indeed critical infrastructure offers an avenue for domestic catastrophic destruction, then the National Protection and Programs Directorate (NPPD) may be considered one of the most important directorates within the Department of Homeland Security (DHS).

The National Protection and Programs Directorate (NPPD) leads national efforts to strengthen the security and resilience of the Nation's critical infrastructure against terrorist attacks, cyber events, natural disasters, other large-scale incidents, and during national security special events.

Background

The National Protection and Programs Directorate traces its lineage to the original Information Analysis & Infrastructure Protection (IA&IP) Directorate. The IA&IP was headed by an Undersecretary supported by two Assistant Secretaries, one for Information Analysis and the other for Infrastructure Protection. The Assistant Secretary for Infrastructure Protection was assigned responsibility for actively protecting the nation's critical infrastructure and developing an overall National Infrastructure Protection Plan (NIPP). [1, pp. 8-9] Responding to Congressional mandates imposed by the 2006 Post-Katrina Emergency Management Reform Act, and using his own authorities under the 2002 Homeland Security Act, in 2007 Secretary Chertoff formed NPPD, headed by an Undersecretary, to consolidate both physical and cyber protection of the nation's critical infrastructure. [2, p. 17]

Mission

The National Protection and Programs Directorate leads national efforts to strengthen the security and resilience of the Nation's critical infrastructure against terrorist attacks, cyber events, natural disasters, other large-scale incidents, and during national security special events. To accomplish its mission, NPPD collaborates with the owners and operators of infrastructure to maintain near real-time situational awareness of both physical and cyber events and share information that may disrupt critical infrastructure. Through partnerships with Federal, State, local, tribal, territorial, international, and private-sector entities, NPPD identifies and enables mitigation and risk reduction to infrastructure and builds capacity to secure the Nation. [3, p. 77]

NPPD works with infrastructure owners and operators, along with others in the private sector; Federal, State, local, territorial, and tribal officials; and international partners to ensure timely information, analysis, and assessments in order to maintain and provide situational awareness, increase resilience, and understand and mitigate risk through its field force and headquarters components. Through established partnerships, NPPD leads the national unity of effort for infrastructure security and resilience and builds capacity of partners across the nation through activities like bombing prevention, technical assistance, training, analysis, and assessments. NPPD also directly protects Federal infrastructure against both physical and cyber threats and responds to incidents which threaten infrastructure at the local level. [3, p. 77]

The goal of the National Protection and Programs Directorate is to advance the Department of Homeland Security's risk-reduction mission. Reducing risk requires an integrated approach that encompasses both physical and virtual threats and their associated human elements.

NPPD leads the national effort for infrastructure security and resilience and builds capacity of partners across the nation.

Organization

The NPPD is organized into five offices:

1. Office of Infrastructure Protection
2. Office of Cybersecurity and Communications
3. Office of Biometric Identity Management
4. Office of Cyber & Infrastructure Analysis
5. Federal Protective Service

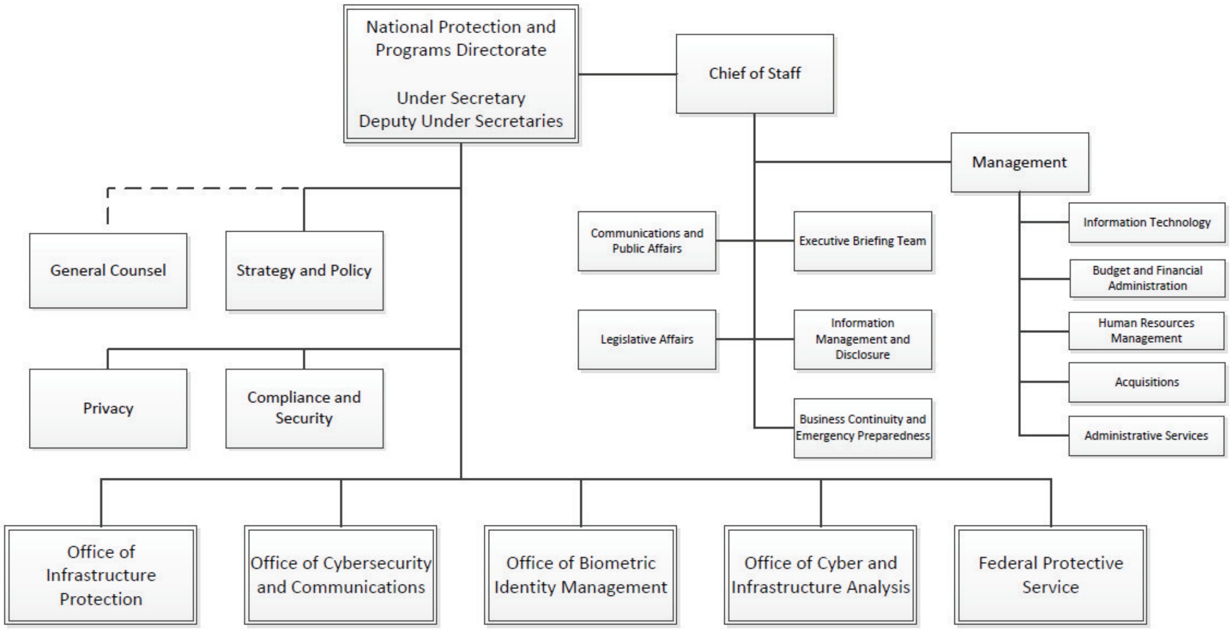
National Protection and Programs Directorate
Under Secretary
Deputy Under Secretaries
Chief of Staff
Management
General Counsel
Strategy and Policy
Communications and Public Affairs
Executive Briefing Team
Information Technology
Budget and Financial Administration
Legislative Affairs
Information Management and Disclosure
Human Resources Management
Privacy
Compliance and Security
Acquisitions
Business Continuity and Emergency Preparedness
Administrative Services
Office of Infrastructure Protection
Office of Cybersecurity and Communications
Office of Biometric Identity Management
Office of Cyber and Infrastructure Analysis
Federal Protective Service

Figure 24-1: NPPD Organization Chart [4]

Office of Infrastructure Protection

The Office of Infrastructure Protection (IP) leads and coordinates national programs and policies on critical infrastructure security and resilience and has established strong partnerships across government and the private sector. The office conducts and facilitates vulnerability and consequence assessments to help critical infrastructure owners and operators and State, local, tribal, and territorial partners understand and address risks to critical infrastructure. IP provides information on emerging threats and hazards so that appropriate actions can be taken. The office also offers tools and training to partners to help them manage the risks to their assets, systems, and networks. [5]

The Office of Infrastructure Protection (IP) leads and coordinates national programs and policies on critical infrastructure security and resilience .

IP's protection efforts are focused on 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. The 16 sectors identified in Presidential Policy Directive 21 (PPD-21) include:

Table 24-1: Critical Infrastructure Sectors

1. Chemical Facilities	9. Financial Services
2. Commercial Facilities	10. Food & Agriculture
3. Communications Assets	11. Government Facilities
4. Critical Manufacturing Facilities	12. Healthcare and Public Health
5. Dams	13. Information Technology
6. Defense Industrial Base	14. Nuclear Reactors, Materials, and Waste
7. Emergency Services	15. Transportation
8. Energy	16. Water and Wastewater Systems

IP's protection efforts are guided by the National Infrastructure Protection Plan. First introduced in 2006, the NIPP was revised in 2009 and again in 2013. The current NIPP advocates protecting critical infrastructure through public/private partnerships predicated on a Risk Management Framework (RMF). The RMF is a 5-step processing for assessing risk and prioritizing countermeasures to reduce the vulnerability of the nation's critical infrastructure. [6]

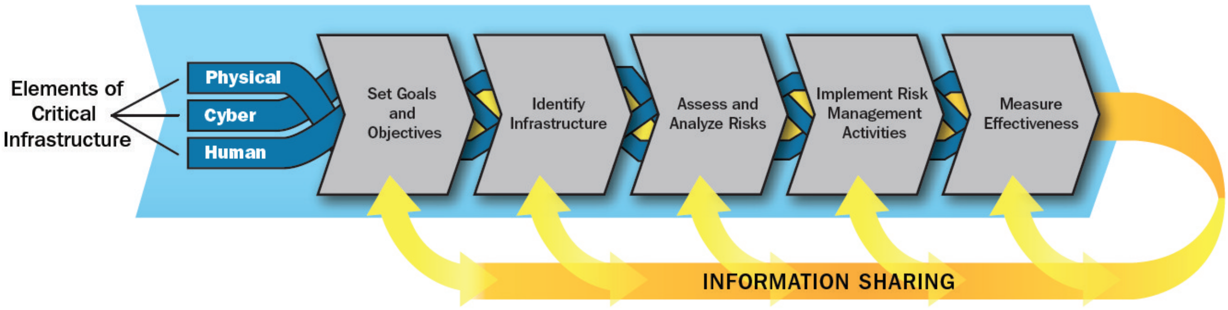

Figure 24-1: NIPP Risk Management Framework [6, p. 15]

The 2013 NIPP represents an evolution from concepts introduced in the initial versions. It is streamlined and adaptable to the current risk, policy, and strategic environments. It provides the foundation for an integrated and collaborative approach to achieve the vision of: "[a] Nation in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened." The 2013 NIPP was developed through a collaborative process involving stakeholders from all 16 critical infrastructure sectors, all 50 states, and from all levels of government and industry. [6]

IP actively monitors the health of the nation's critical infrastructure through the National Infrastructure Coordinating Center (NICC). The NICC is an element of the Department's National Operations Center (NOC) which maintains active watch over all homeland security threats. When an incident or event impacting critical infrastructure occurs that requires coordination between DHS and the owners and operators of critical infrastructure, the NICC is the national coordination hub to support the security and resilience of physical critical infrastructure assets. The NICC collaborates with Federal departments, State and Local governments, and private sector partners to monitor potential, developing, and current regional and national operations of the Nation's critical infrastructure sectors. [7, p. 1]

IP actively monitors the health of the nation's critical infrastructure through the National Infrastructure Coordinating Center (NICC). Similarly, the National Cybersecurity and Communications Integration Center (NCCIC) stands watch for national cyber threats.

Similarly, the National Cybersecurity and Communications Integration Center (NCCIC) stands watch for national cyber threats. It issues alerts and coordinates response through law enforcement agencies, the Intelligence Community (IC), international computer emergency readiness teams, domestic Information Sharing And Analysis Centers (ISACs), and critical infrastructure partners. [7, p. 2]

Both the NICC and NCCIC maintain active relationships with Federal partners, law enforcement, and emergency management communities. Other government agencies also work with the NICC and NCCIC and share interest in critical infrastructure-related information. For example, the NICC works closely with the State Department's Overseas Security Advisory Council, which provides information regarding threats to physical infrastructure overseas to American organizations and can ensure this information is available to the domestic critical infrastructure community. At the same time, the NCCIC works on a daily basis with other Federal cyber centers to exchange critical information and coordinate analytical and response processes. Both centers provide reports to the National Operations Center to facilitate shared situational awareness across the Federal community. [7, pp. 4-5]

Important components of the NCCIC include the United States Computer Emergency Readiness Team (US-CERT) and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). They maintain web-based, collaborative tools to share sensitive cybersecurity prevention, protection, mitigation, response, and recovery information with validated partners. They provide access to a secure portals which provides information regarding cyber indicators, incidents, advisories, and malware digests for critical infrastructure systems. [7, p. 3]

- The Cobalt Compartment is an information hub for enterprise systems security.
- The Control System Compartment provides material on industrial control systems, limited to control system asset owners and operators.
- A National Cyber Awareness System provides timely alerts, bulletins, tips, and technical documents to those who sign up.
- Cybersecurity incident reporting provides critical infrastructure partners with a secure means to report cybersecurity incidents.

The Infrastructure Information Collection Division (IICD) within the NPPD's Office of Infrastructure Protection (IP) leads the Department's efforts to gather and manage vital information regarding the nation's critical infrastructure.

The Infrastructure Information Collection Division (IICD) within the NPPD's Office of Infrastructure Protection (IP) leads the Department's efforts to gather and manage vital information regarding the nation's critical infrastructure. The Web-based infrastructure surveys and assessments, available through the Infrastructure Protection (IP) Gateway, allow users to capture valuable data on a facility's physical and operational security and its resilience to attacks and natural hazards. The collected data is analyzed to determine the facility's relative security and resilience in comparison to the national average for similar facilities. This information is used to develop dashboards that equip the facility's owners and operators with the knowledge to detect and prevent physical, cyber, and natural threats, and better respond to, recover from, and remain resilient against all hazards. [8]

To enhance information-sharing efforts among the public and private sectors, the Protected Critical Infrastructure Information (PCII) program provides congressionally mandated protections from public disclosure to qualifying critical infrastructure information. The success of the nation's collaborative critical infrastructure protection program relies on participation from critical infrastructure owners and operators. The PCII program supports this effort by providing owners and operators with the assurance that their sensitive information can be protected. [8]

To support the efforts of critical infrastructure planners and other IP mission partners, IICD has integrated data visualization and mapping capabilities within the IP Gateway. The secure, web-based, geospatial mapping tool integrates commercial and government-owned data and imagery from multiple sources, to support complex data analysis or provide comprehensive situational and strategic awareness. [8]

The OneView program is also available as an alternative visualization capability for Geospatial Information Infrastructure (GII). OneView provides a rich interface for viewing maps of critical infrastructure, natural hazards data, and other user defined data sources, as well as enhanced imagery, geocoding, and routing features. [8]

IICD manages infrastructure information partnerships with homeland security geospatial stakeholders in state and local governments, as well as the private sector. These partnerships include activities such as working to define better geospatial information requirements and to improve data sharing, creating geospatial data sets for partner use, assigning staff to work in the field and serve as focal points for state and local data needs, and managing workshops to address future geospatial information issues in homeland security and emergency response. [8]

The Office of Cybersecurity and Communications (CS&C) is responsible for enhancing the security, resilience, and reliability of the Nation's cyber and communications infrastructure.

Office of Cybersecurity and Communications

The Office of Cybersecurity and Communications (CS&C) is responsible for enhancing the security, resilience, and reliability of the Nation's cyber and communications infrastructure. CS&C works to prevent or minimize disruptions to critical information infrastructure in order to protect the public, the economy, and government services. CS&C leads efforts to protect the federal ".gov" domain of civilian government networks and to collaborate with the private sector—the ".com" domain—to increase the security of critical networks. [9]

Within CS&C is the Office of Emergency Communications (OEC). Established in 2007 in response to communications challenges faced during the attacks on September 11, 2001 and Hurricane Katrina, the OEC supports and promotes communications used by emergency responders and government officials to keep America safe, secure, and resilient. The office leads the Nation's operable and interoperable public safety and national security and emergency preparedness (NS/EP) communications efforts. OEC provides training, coordination, tools, and guidance to help its federal, state, local, tribal, territorial and industry partners develop their emergency communications capabilities. OEC's programs and services coordinate emergency communications planning, preparation and evaluation, to ensure safer, better-prepared communities nationwide.

CS&C coordinates national security and emergency preparedness through the Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR) office. CS&C relies on SECIR to streamline coordination and engagement with external partners, while leveraging capabilities and significant subject matter expertise in order to meet stakeholder requirements.

The Federal Network Resilience (FNR) office within CS&C is responsible for developing metrics to drive cybersecurity risk management for Federal departments and agencies. FNR also gathers cybersecurity requirements and develops operational policies for the Federal government. It collaborates with, and provides outreach to, the Office of Management and Budget (OMB), the Federal Chief Information Officer (CIO) Council, and individual agency Chief Information (CIOs) and Chief Information Security Officers (CISOs) of various Federal agencies. FNR is a clearing house for cyber best practices and cyber lessons learned in support of Federal departments and agencies.

The CS&C Network Security Deployment (NSD) office works collaboratively with public, private, and international entities to secure cyberspace and America's cyber assets. NSD serves as the cybersecurity engineering and acquisition "Center of Excellence" within CS&C. In support of that role, NSD provides development, acquisition, deployment, operational, and customer support to satisfy the Department's mission requirements under the Comprehensive National Cybersecurity Initiative (CNCI). [9]

Finally, CS&C operates the Enterprise Performance Management Office (EPMO), which ensures that the Assistant Secretary's strategic goals and priorities are reflected across all CS&C programs. EPMO measures the effectiveness of initiatives, programs, and projects that support those goals and priorities, and facilitates cross-functional mission coordination and implementation between CS&C components within DHS, and among the interagency. [9]

The Office of Biometric Identity Management (OBIM) is responsible for collecting, maintaining, and sharing biometric data with the law enforcement and intelligence communities and strategic foreign partners. As part of this mission, it maintains the Automated Biometric Identification System (IDENT)—DHS's central repository for biometric data.

Office of Biometric Identity Management (OBIM)

The Office of Biometric Identity Management (OBIM) is responsible for collecting, maintaining, and sharing biometric data with the law enforcement and intelligence communities and strategic foreign partners. As part of this mission, it maintains the Automated Biometric Identification System (IDENT)—DHS's central repository for biometric data. [10, p. 11] OBIM was created in March, 2013, replacing the United States Visitor and Immigration Status Indicator Technology (US-VISIT) Program, the system used by the DHS for keeping track of all visitors to the country and checking all of their identity through various biometric technologies. [11]

Formerly US-VISIT, the OBIM uses biometrics to help make travel simple, easy and convenient for legitimate visitors, but virtually impossible for those who wish to do harm or violate U.S. laws. Biometrics collected by OBIM and linked to specific biographic information enable a person's identity to be established, then verified, by the U.S. government. With each encounter, from applying for a visa to seeking immigration benefits to entering the United States, OBIM:

Checks a person's biometrics against a watch list of known or suspected terrorists, criminals and immigration violators

Checks against the entire database of all of the fingerprints the Department of Homeland Security has collected since OBIM began to determine if a person is using an alias and attempting to use fraudulent identification.

Checks a person's biometrics against those associated with the identification document presented to ensure that the document belongs to the person presenting it and not someone else. [12]

OBIM provides the results of these checks to decision makers when and where they need it. These services help prevent identity fraud and deprive criminals and immigration violators of the ability to cross U.S. borders. Based on biometrics alone, OBIM has helped stop thousands of people who were ineligible to enter the United States. Biometrics are unique physical characteristics, such as fingerprints, that can be used for automated recognition. Biometrics form the foundation of OBIM's identification services because they are reliable, convenient and virtually impossible to forge. [12]

The Office of Cyber & Infrastructure Analysis (OCIA) performs integrated analysis of critical infrastructure, and identifies critical infrastructure where cyber incidents could have catastrophic impacts. To assist with these responsibilities, the OCIA manages the National Infrastructure Simulation and Analysis Center (NISAC) on Kirtland Air Force Base in Albuquerque, NM.

Privacy is an integral part of the OBIM and it is essential to the program mission. OBIM takes privacy into account from conception through planning and development, and during the execution of every aspect of the OBIM program. Personal information collected by OBIM is to be used only for the purposes for which it was collected, unless specifically authorized or mandated by law. OBIM has carefully monitored systems and security practices in place to protect the privacy of those whose data are collected and to ensure the integrity of that data. OBIM has dedicated privacy personnel to further ensure that the information collected is protected from misuse by anyone inside or outside OBIM. [12]

Office of Cyber & Infrastructure Analysis

Formerly the Infrastructure Analysis and Strategy Division (IASD) within the Office of Infrastructure Protection (IP), OCIA was established as an office of the NPPD in 2014. OCIA has an important role in DHS's efforts to implement Presidential Policy Directive 21 (PPD-21), which calls for integrated analysis of critical infrastructure, and Executive Order 13636, identifying critical infrastructure where cyber incidents could have catastrophic impacts to public health and safety, the economy, and national security.

OCIA builds on the recent accomplishments of the Department's Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) and manages the National Infrastructure Simulation and Analysis Center (NISAC) to advance understanding of emerging risks crossing the cyber-physical domain. OCIA represents an integration and enhancement of DHS's analytic capabilities, supporting stakeholders and interagency partners.

Federal Protective Service

The Federal Protective Service (FPS), within the National Protection and Programs Directorate is responsible for the protection and security of federal property, personnel, and federally owned and leased buildings. In general, FPS operations focus on security and law enforcement activities that reduce vulnerability to criminal and terrorist threats. FPS protection and security operations include all-hazards based risk assessments; emplacement of criminal and terrorist countermeasures, such as vehicle barriers and closed-circuit cameras; law enforcement response; assistance to federal agencies through Facility Security Committees; and emergency and safety education programs. FPS also assists other federal agencies, such as the U.S. Secret Service (USSS) at National Special Security Events (NSSE), with additional security. FPS is the lead "Government Facilities Sector Agency" for the National Infrastructure Protection Plan (NIPP). There are more than 1,300 Law Enforcement Officers, Security Specialists, Special Agents and Mission Support Staff protecting federal facilities and tenants (4) along with approximately 13,000 contract security guards. [10, p. 10]

The Federal Protective Service (FPS), within NPPD is responsible for the protection and security of federal property, personnel, and federally owned and leased buildings.

The Federal Protective Service provides integrated security and law enforcement services to more than 9,500 federal facilities nationwide. These services include: conducting facility security assessments; responding to crimes and other incidents to protect life and property; and detecting, investigating, and mitigating threats. [13] Protective services of the FPS also include:

- Designing countermeasures for tenant agencies
- Maintaining uniformed law enforcement presence
- Maintaining armed contract security guards
- Performing background suitability checks for contract employees
- Offering special operations including K-9 explosive detection
- Monitoring security alarms via centralized communication centers
- Sharing intelligence among local/state/federal
- Protecting special events
- Training federal tenants in crime prevention and occupant emergency planning

In the spring of 2013, the Federal Protective Service (FPS) implemented a new directive entitled the Prohibited Items Program (FPS Directive 15.9.3.1. (Rev. 1). The Prohibited Items Program sets forth FPS' policy for applying security force countermeasures to mitigate prohibited item entry at Federal properties. The intent of the policy is to provide risk-based recommendations to Facility Security Committees regarding security screening, visitor processing, and the development of prohibited items lists and accommodation policies as well as establishing FPS policies and procedures for addressing prohibited items. The Facility Security Committee is responsible for determining the security countermeasures and prohibited item list for a particular Federal facility. FPS is responsible for implementing the security countermeasures and enforcing the prohibited items list developed by the Facility Security Committee.

Within the Federal Protective Service, the Office for Bombing Prevention (OBP) leads the DHS's efforts to implement the National Policy for Countering Improvised Explosive Devices (IED) and enhance the nation's ability to prevent, protect against, respond to, and mitigate the use of explosives against critical infrastructure; the private sector; and federal, state, local, tribal, and territorial entities. OBP was born of terrorism events, such as Lockerbie, Oklahoma City, 9/11, Madrid, and London through its mission to protect life and critical infrastructure by building capabilities within the general public and across the public and private sectors to prevent, protect against, respond to, and mitigate bombing incidents. [14]

The FPS also has other specialized capabilities. FPS Explosive Detection Canine (EDC) teams conduct searches for a variety of explosive materials near building exteriors, parking lots, office areas, vehicles, packages, and people in and around Federal facilities. They also provide a strong visible and psychological deterrent against criminal and terrorist threats. The teams are available to assist federal, state, and local law enforcement partners. EDC teams play a critical role in FPS' comprehensive preventive security measures by supporting strategic explosive detection activities. They also provide immediate and specialized response to bomb threats and unattended packages or other such dangerous items. Most often, these detection activities allow the EDC teams to detect or quickly rule out the presence of dangerous materials and allow the business of the government to continue with minimal or no interruption. FPS has also initiated a Personnel Screening Detection (PSD) program. PSD canines are specially trained to detect explosives carried by people or in moving containers, such as luggage or backpacks. [13]

Within the Federal Protective Service, the Office for Bombing Prevention (OBP) leads the DHS's efforts to implement the National Policy for Countering Improvised Explosive Devices (IED).

FPS mobile command vehicles (MCV) are deployed to enhance or reestablish communication and coordination during emergency incidents and special security events nationwide. These assets leverage satellite and internet access, as well as interoperable radios and video capabilities to enhance communication between FPS assets and other federal and local response and support assets. The MCVs can rapidly deploy to any location in the continental United States where the communications infrastructure is inadequate or has been disrupted, or where enhanced interoperability among law enforcement agencies is needed.

Conclusion

While, arguably, NPPD may have the most important job in DHS, without doubt it also has one of the most challenging jobs in DHS. Critical infrastructure protection remains a work in progress. Although DHS has succeeded in engaging owners and operators in a dialog about critical infrastructure protection, it has made little progress in actually reducing vulnerabilities as the Department was tasked to do by the 2002 Homeland Security Act. In part, the predicament is the result of an absence of workable solutions. Critical infrastructure protection is a job easier said than done. This assessment is evidenced by 1) the Department's inability to compile a definitive list of critical infrastructure, 2) develop a transparent and

Challenge Your Understanding

The following questions are designed to challenge your understanding of the material presented in this chapter. Some questions may require additional research outside this book in order to provide a complete answer.

1. What is the mission of the National Protection and Programs Directorate?
2. Which NPPD component has primary responsibility for critical infrastructure protection?
3. Which NPPD component monitors the nation's infrastructure?
4. Which NPPD component stands watch for national cyber threats?
5. Which NPPD component collects and manages information about critical infrastructure?
6. Which NPPD component is responsible for protecting the ".gov" Internet domain?
7. Which NPPD component collects and manages law enforcement biometric data?
8. Which NPPD component performs integrated analysis of critical infrastructure?
9. Which NPPD component performs modeling and simulation of critical infrastructure?
10. Which NPPD component works to counter improvised explosive devices?