

DHS Transition Issue Paper

Cybersecurity Responsibilities and Authorities

OVERVIEW

- Cyber threats continue to grow and evolve at a rapid pace. Such threats are seen across Government networks and all U.S. critical infrastructure sectors, including the Financial Services, Energy, Transportation, Emergency Services, Information Technology, Communications, and Healthcare and Public Health sectors. Potential impacts from cyber incidents include data corruption, data theft, and physical consequences.
- DHS has broad cybersecurity responsibilities and authorities, including responsibility to protect the Federal civilian government, enhance the security and resilience of critical infrastructure, investigate, disrupt, and deter cyber crimes, respond to incidents, share cybersecurity information and improve the overall cyber ecosystem. DHS is directed, in multiple laws and executive orders (EOs), to conduct these missions in a manner that respects privacy and civil liberties.
- The *2014 Quadrennial Homeland Security Review*¹ identifies “Safeguarding and Securing Cyberspace” as one of five core DHS mission areas. The Office of Policy (PLCY) is responsible for developing DHS-wide strategic approaches across the cybersecurity mission.

DETAILED DISCUSSION

DHS Cybersecurity Roles and Responsibilities

- *Protect federal civilian government.* The National Protection and Programs Directorate (NPPD) leads efforts to provide a common baseline of security across the federal executive branch civilian agencies and assist other federal and non-federal entities manage their cyber risk while MGMT is responsible for security the Department’s own networks.
 - This common baseline is principally provided by two programs: the EINSTEIN program, which detects and blocks cyber attacks outside of agency perimeters, and the Continuous Diagnostics and Mitigation (CDM) program, which provides tools for agencies to identify and prioritize vulnerabilities within their networks.
 - All agencies are required to participate in EINSTEIN by December 18th, 2016. DHS has provided the first phase of CDM, while the second and third phases will be deployed over the next two fiscal years.
- *Enhance the security and resilience of the nation’s physical and cyber infrastructure.* NPPD serves as the national coordinator across all 16 critical infrastructure sectors, enabling situational awareness, building partner capacity to manage risk, and directly protecting infrastructure, particularly federal executive branch civilian networks. NPPD’s cybersecurity mission is not confined to critical infrastructure.
 - PLCY, NPPD, and S&T are working together on guidance regarding best practices for the systems, networks, and devices that make up the Internet of Things.
- *Investigating, disrupting, and deterring cybercrimes.* USSS and Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) have broad criminal jurisdiction to investigate cyber crimes within their areas of responsibility.

¹ <https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf>

- ICE HSI focuses on border enforcement related crimes, including intellectual property rights violations, child exploitation, trade restricted data, and cross-border smuggling.
- USSS combats electronic crimes that impact U.S. financial and payment systems as well as illegal computer intrusions or frauds that violate 18 U.S.C. § 1030.
- USSS deters cybercrime by partnering with state and local law enforcement counterparts through its network of Electronic Crimes Task Forces and by training state and local law enforcement, prosecutors, and judges at the National Computer Forensics Institute.
- *Respond effectively to cyber incidents.* NPPD, through the National Cybersecurity and Communication and Integration Center (NCCIC), provides on-site incident response and other technical assistance, enhances reporting capabilities and relationships, and tracks, identifies and assesses overall trends and connections.
 - USSS leads investigative efforts focused on financial crimes, and ICE/HSI performs related cyber investigations and forensics in the field and from their Cyber Crimes Center. In the case of significant cyber incidents for which a Cyber UCG is created, USSS and ICE/HSI will closely coordinate their threat response activities with the DOJ and the Cyber UCG.
- *Share timely and actionable cybersecurity information.* DHS shares timely and actionable cybersecurity information to enable the protection of infrastructure and better respond to incidents.
 - The NCCIC serves as the federal-civilian interface for cybersecurity information sharing and provides cybersecurity related technical assistance, risk management support, and incident response capabilities to federal and non-federal entities.
 - NPPD is expanding automated, real-time sharing of cyber threat indicators through the Automated Indicator Sharing capability required under the Cybersecurity Information Sharing Act of 2015 (Title I of the Cybersecurity Act of 2015 or CISA).
 - NPPD is also supporting the development of Information Sharing Analysis Centers and Information Sharing and Analysis Organizations in accordance with EO 13691.
 - USSS and ICE HSI continue to share information about cyber investigation and crimes with the NCCIC and appropriate partners through Electronic Crimes Task Forces and other existing mechanisms.
- *Improve the cyber ecosystem through best practices, research and development, international engagement, education and training.*
 - NPPD works to shape the IT market so that systems are more secure. This includes driving developers to implement best practices and fostering a market for interoperable security products that will enable small and medium businesses to secure themselves.
 - S&T coordinates internal and external RDT&E by DHS, the Federal government and Industry organizations, to support DHS operational priorities and help strengthen associated cybersecurity outcomes, including network defense, law enforcement investigative and forensics capabilities, and many different collaboration approaches to leverage national innovation resources for Homeland Security Enterprise gain.
 - PLCY leads efforts to expand bilateral and multilateral international engagements to advance goals of an open, interoperable, secure and reliable Internet that enables trade and the freedom of expression, while protecting the privacy and security of its users; and
 - NPPD supports capacity building efforts with international partners, including the development of Computer Security Incident Response Teams, supports the National

Initiative on Cybersecurity Education, and works with S&T, academia, and industry to pilot innovative cybersecurity technologies.

- MGMT works will all components to improve cyber recruitment, education and training to ensure skilled cyber workforce for DHS and whole of Nation.

Authorities of DHS in Cybersecurity

- The National Cybersecurity Protection Act of 2014 codified and expanded the authorities and responsibilities of the National Cybersecurity and Communications Integration Center (NCCIC) to focus on threats and incidents that impact critical infrastructure and beyond and authorized the NCCIC as the civilian hub for sharing cyber threat indicators and defensive measures with and among federal and non-federal entities, including the private sector.
- The Federal Information Security Modernization Act of 2014 (FISMA) establishes DHS's central role in the security of the information and information systems of federal executive branch civilian agencies. Through NPPD, DHS administers the implementation of government-wide policies, deploys technologies to assist in the protection of federal agencies' networks, and issues binding operational directives to agencies to safeguard information and information systems.
- CISA requires the Department, in consultation with interagency partners, to establish a capability and process for sharing cyber threat indicators with both federal and private sector entities. It directs DHS to share cyber threat indicators and defensive measures in an automated and real-time manner. The law provides targeted liability protection to companies that share cyber threat indicators with DHS and provides other legal protections for indicators shared in accordance with CISA. Finally, the law authorizes private entities to monitor their networks for cybersecurity threats and operate defensive measures, with liability protection for doing so.
- The Federal Cybersecurity Enhancement Act of 2015 (Title II, Subtitle B of the Cybersecurity Act of 2015) establishes DHS's NCCIC as the central hub for the sharing of cyber threat indicators between the private sector and the federal government. The law also authorizes DHS's EINSTEIN capability for the protection of federal networks and requires federal agencies to implement it by December 18, 2016.
- EO 13636—*Improving Critical Infrastructure Cybersecurity* and Presidential Policy Directive (PPD) 21—*Critical Infrastructure Security and Resilience*² direct the Department to develop and implement strategic approaches to increase situational awareness of physical and cyber threats to infrastructure, and reinforces the need for holistic thinking about security and risk management.
- EO 13691—*Promoting Private Sector Cybersecurity Information Sharing*³ (2015), tasks DHS with encouraging the development and formation of Information Sharing and Analysis Organizations (ISAOs) and entering into an agreement with a nongovernmental organization to serve as the ISAO Standards Organization to identify a common set of voluntary standards or guidelines for the creation and functioning of ISAOs under the EO.
- PPD 41—*Cyber Incident Coordination Policy*⁴, sets forth principles governing the federal government's response to any cyber incident and, for significant cyber incidents, establishes

² <https://www.dhs.gov/sites/default/files/publications/EO-13636-PPD-21-Fact-Sheet-508.pdf>

³ <https://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf>

an architecture for coordinating the broader response and recovery efforts, through a Cyber Unified Coordination Group (Cyber UCG) with lead federal agencies responsible for coordinating respective lines of effort.

- During a significant incident, DHS, acting through the NCCIC, is the federal lead agency for asset response activities. DHS also takes information from a given incident and shares it broadly, so that others will be protected against the same or similar incidents.
 - During a significant incident, DOJ, acting through the Federal Bureau of Investigation and the National Cyber Investigative Joint Task Force, is the federal lead agency for threat response activities. USSS and ICE HSI are responsible for investigating cyber crimes within their jurisdiction and if a Cyber UCG is formed, will coordinate their threat response activities with DOJ.
 - The Office of the Director of National Intelligence, through the Cyber Threat Intelligence Integration Center, is the federal lead agency for intelligence support and related activities.
 - The Directive requires DHS to lead the development of the National Cyber Incident Response Plan.
- Consistent with 18 U.S.C. § 3056(a), the USSS assesses and mitigates cybersecurity risks to systems that could impact the agency’s protective mission. The USSS also has explicit authority to investigate access-device and computer fraud offenses. For example, the USSS investigates cyber crimes that have a significant economic or community impact, involve organized criminal groups or international organizations, or involve novel misuses of information technology.
 - The USA PATRIOT Act of 2001 (Pub.L 107-56, Sec. 105, 18 U.S.C. § 3056 note) requires the USSS “to develop a national network of electronic crime task forces, based on the New York Electronic Crimes Task Force model, throughout the United States, for the purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems.”
 - HSI Special Agents, as Immigration and Customs Criminal Investigators, investigate violations of criminal laws found in Titles 8, 18, 19, 21, 22, 31, 46 and 50 of the U.S. Code, including situations in which computers are used in the commission of those crimes, the digital theft of intellectual property and export controlled data. When charges or potential charges are being considered pursuant to a criminal investigation, HSI will, as appropriate, include violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.
 - The Human Exploitation Rescue Operations (HERO) Act of 2015 amends the Homeland Security Act and directs the Department to operate, within HSI, a Cyber Crimes Center to provide investigative assistance, training and equipment to support domestic and international investigations by HSI of cyber-related crimes. 6 U.S.C. § 473(a). The law also codifies HSI’s specific cybercrime and cybersecurity authorities by creating a Cyber Crimes Unit (CCU) within the Cyber Crimes Center, which oversees the cyber security strategy and cyber related operations and programs for HSI. 6 U.S.C. § 143(d).
 - The United States Coast Guard (USCG) serves as the Sector Specific Agency (as defined by the National Infrastructure Protection Plan) for the Maritime Transportation Subsector (delegated by DHS). USCG has certain authorities over regulated facilities and vessels.

⁴ <https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>

Through the Captain of the Port (COTP) and Officer in Charge, Marine Inspection (OCMI), the USCG is working to integrate cyber threats into its regulatory regime.

Courses of Action

- Cross-Departmental policy development and coordination
 - PLCY leads development of cross-Departmental strategy, policy and plans in coordination with other DHS components.
 - Current areas of focus include encryption, cyber export controls, engagement with countries of interest, implementation of presidential directives, and ensuring a whole of DHS approach to cyber issues.
- NPPD Transformation Planning
 - NPPD currently undertakes strategic and operational activities to help critical infrastructure owners and operators manage all-hazards risk. But NPPD's name and structure do not reflect this conjoined mission or its increasingly operational responsibilities.
 - NPPD's transition plan seeks to address the growing threat to U.S. critical infrastructure from cyber and other means by taking an operationally focused and integrated approach across "cyber" and "infrastructure" protection in order to recommend or implement effective cybersecurity measures.
 - The Department is working with Congress to ensure that NPPD is provided with a name, "*Cyber and Infrastructure Protection Agency*," or CIP, that reflects its broad responsibilities, and that the Secretary is authorized to implement an organizational structure that reflects the all-hazards nature of NPPD's mission.
- Implementation of PPD-41
 - NPPD will continue to mature the government's execution of incident coordination functions provided by PPD-41, including the development and issuance of the National Cyber Incident Response Plan.
 - NPPD, USSS, and USCG will develop the required enhanced coordination procedures to guide their operational actions during significant cyber incidents.
 - PLCY will coordinate with other DHS components to ensure consistency in approach.
- Deployment of EINSTEIN Capabilities
 - Federal departments and agencies are statutorily required to implement existing EINSTEIN capabilities by December 2016.
 - NPPD will continue to work with outstanding departments and agencies.
- Automated Indicator Sharing
 - NPPD will continue to expand and refine the information sharing capabilities mandated by CISA by signing up additional participating entities to submit and receive threat indicators.

Key Partnerships

- DHS, through NPPD and other components, partners with private sector and governmental infrastructure owners and operators, manufacturers, and/or service providers to improve the security and resilience of existing infrastructure and new technology products against a growing range of cyber threats. DHS has built a number of public-private partnership mechanisms to enable trusted, bi-directional information sharing relationships with its partners and to address and mitigate vulnerabilities and incidents. Most DHS cybersecurity RDT&E efforts also involve industry collaboration.

- DHS is actively working on engagement and educational efforts within various stakeholders that include tailored information sharing, analytical products, and risk assessments.
- Cyber and cyber-enabled threats increasingly originate outside the geographic boundaries of the homeland, the Department will continue to develop and expand operational and R&D relationships with international partners to mitigate the risk from foreign elements.

DHS Transition Issue Paper

Emergency Authorities of the Secretary of Homeland Security

OVERVIEW

- The Secretary of Homeland Security has broad legal authorities to take actions to secure the Nation's borders, its waterways and coasts, and its transportation systems. During a domestic incident, such as a natural disaster, terrorist attack, or other emergency, the Secretary and the Department have additional responsibilities and authorities to augment their broad, standing homeland security authorities.
- This paper provides a high-level description of the actions the Secretary must or may take in response to an emergency situation. It first describes the emergency response roles of the Secretary and the Administrator of the Federal Emergency Management Agency (FEMA) and also provides an illustrative, non-exhaustive summary of key authorities underlying the Secretary's responsibilities and authorities during a domestic incident.
- The U.S. disaster relief system gives state, local, tribal, and territorial (SLTT) governments, not the Federal government, primary authority and responsibility for conducting response and recovery activities. Subject to limited exceptions of special Federal interest (e.g., Federal actions in response to a potential or actual Federal crime of terrorism), the Federal government's role in emergency response is to provide support and assistance to SLTT efforts. Several Federal statutes provide additional authority to the Federal government when SLTT governments are overwhelmed by an incident. This paper outlines the key authorities by which the Secretary provides assistance to state and local governments and, where appropriate, the Secretary takes a lead role in national-level decision-making as part of the overall response to an incident.
- Additionally, other Federal departments and agencies may assume a lead role in an overall Federal response, depending on the facts, circumstances, and legal authorities applicable to a particular incident. In such cases, and depending on the circumstances, the Secretary may provide personnel, technical assistance, or other support to that department or agency serving as the overall Federal lead in responding to an incident.

DETAILED DISCUSSION

The Roles of DHS Officials in Emergency Response

- *Role of the Secretary of Homeland Security in Domestic Incident Management.* As the focal point for crises and emergency planning and the principal Federal official for domestic incident management, the Secretary is responsible for coordinating preparedness activities and operations within the United States to respond to and recover from terrorist attacks, major disasters, and other emergencies.
 - *Coordination of Federal Resources.* Pursuant to Homeland Security Presidential Directive 5, the Secretary is responsible for coordinating the Federal government's resources utilized in response to or recovery from major disasters or other emergencies if and when

any one of the following conditions is satisfied: (1) a Federal department or agency acting under its own authority has requested the assistance of the Secretary; (2) the resources of state and local authorities are overwhelmed and Federal assistance has been requested by the appropriate state and local authorities; (3) more than one Federal department or agency has become substantially involved in responding to the incident; or (4) the Secretary has been directed to assume responsibility for managing the domestic incident by the President.

- *Role of FEMA and the FEMA Administrator.* FEMA’s mission is to reduce the loss of life and property and protect the Nation from all hazards, including natural disasters, acts of terrorism, and other man-made disasters, by leading and supporting the Nation in a risk-based, comprehensive emergency management system of preparedness, protection, response, recovery, and mitigation. The Administrator has broad authorities and significant capabilities to carry out this mission and fulfills a statutory role as the principal advisor to the President, National Security Council, and Secretary for all matters relating to emergency management in the United States.
 - *Lead the Nation’s Efforts.* The Administrator leads the Nation’s efforts to prepare for, protect against, respond to, recover from, and mitigate against the risk of natural disasters, acts of terrorism, and other man-made disasters, including catastrophic incidents.
 - *Assist the President.* The Administrator is responsible for assisting the President in carrying out the functions under the Stafford Act (see below) and carrying out all functions and authorities assigned to the Administrator under the Stafford Act.

Key DHS Authorities in Emergency Response

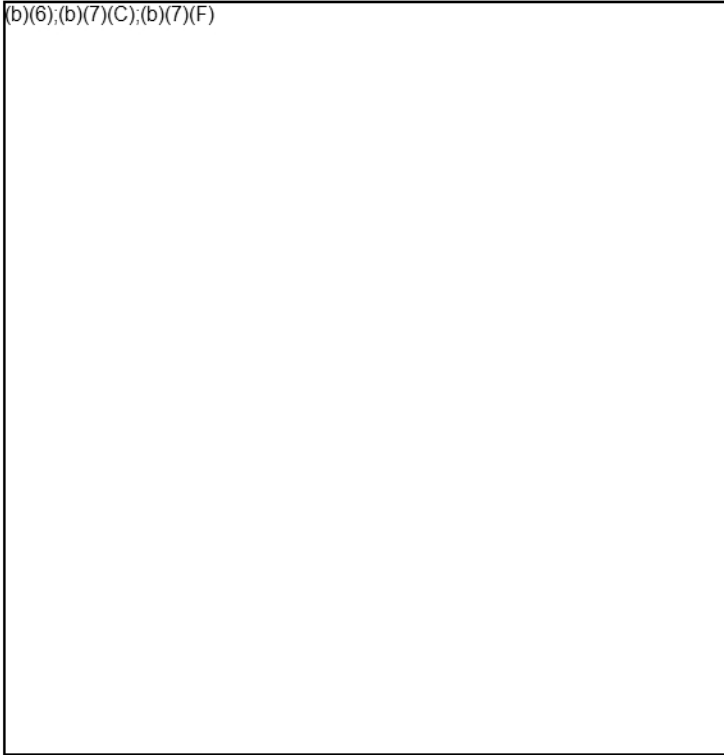
- Because the authorities utilized in the Department’s response to a particular emergency depend on the facts and circumstances underlying the specific incident, the authorities discussed below may or may not be applicable to a particular type of event (i.e., a significant cybersecurity incident versus a hurricane or other natural disaster). In any event, the Secretary may invoke his non-emergency authorities in support of the Federal response.
 - *Stafford Act Assistance.* Following a Presidentially-declared “major disaster” or “emergency,” the Stafford Act is the primary statutory mechanism for providing Federal assistance to SLTT governments. Under the the Stafford Act, the President may issue “major disaster” or “emergency” declarations upon the request of a state or territorial governor or chief tribal executive in response to incidents that overwhelm SLTT governments. These declarations enable the Federal government, through FEMA, to pre-position and surge resources, as well as provide a wide range of financial assistance to individuals and families, certain non-profit organizations, and SLTT governments. Additionally, these declarations enable FEMA to direct Federal assistance to SLTT governments for emergency protective measures. A major disaster declaration may authorize comprehensive Stafford Act assistance, whereas an emergency declaration provides only a limited scope of Federal assistance. FEMA also has authority to take proactive steps in anticipation of incidents and absent a SLTT request.
 - *Public Communications.* The Secretary is responsible for ensuring that, as appropriate, information related to domestic incidents is gathered and provided to the public, the private sector, SLTT authorities, Federal departments and agencies, and the President. For

example, in response to a domestic terrorist threat or attack, the Secretary may utilize the National Terrorism Advisory System to alert stakeholder communities of interest and the public of credible, specific terrorist threats and to recommend protective measures based on the nature of the threat.

- *Maritime Authorities.* The Secretary, through the U.S. Coast Guard, has legal authority to ensure the safety and security of vessels and waterfront facilities and manage the Nation's navigable waterways. Coast Guard officials have broad authority, usually exercised by officials designated as Captains of the Port, to control ports and vessels. The Captains of the Port can use these authorities to control, direct, and should the situation dictate, restrict the flow of maritime traffic into, out of, and within a specific area, as necessary.
- *Transportation Authorities.* The Secretary, through the Transportation Security Administration (TSA), has broad authority to order security enhancements at airports and other key transportation sites and systems. This includes the authority to order the cessation of specific flights or categories of flights, including those arriving from or departing to foreign countries. The TSA Administrator also has substantial authority to enhance the security of railways and mass transit systems.
- *Security and Control Measures at Ports of Entry.* The Secretary, through U.S. Customs and Border Protection, may implement any number of measures to control the movement of people, vehicles, and conveyances at ports of entry. The Secretary may close and consolidate ports of entry, or take other actions at ports of entry necessary to respond to a threat. The Secretary may also rely upon his broad authority to designate other Federal, state, and international agency personnel as customs officers, to demand assistance from any person to enforce customs laws, to authorize other Federal personnel to act with all the powers, privileges, or duties of immigration officers, and in certain circumstances, to authorize state and local law enforcement officers to assist in Federal immigration enforcement.
- *Cyber Incident Response and Critical Infrastructure Protection.* The Secretary, through the National Protection and Programs Directorate, coordinates the Federal government's response to significant cyber incidents that impact critical infrastructure. The Department is the lead Federal agency for so-called "asset response activities." These activities include furnishing technical assistance to affected entities (both governmental and private sector) and identifying other entities that may be at risk, during significant cyber incidents. The Department also serves as the primary Federal agency responsible for developing plans for and coordinating the national effort to protect critical infrastructure in the United States.
- *Continuity of Operations and Continuity of Government.* During a crisis, the Federal government may implement measures to ensure that its mission essential functions continue to be performed during a wide range of emergencies. The Secretary, through the FEMA Administrator, serves as the President's lead agent for coordinating overall continuity operations and activities of Executive Branch departments and agencies, and the Administrator is responsible for preparing and implementing the Federal government's continuity plans and programs.

National Protection and Programs Directorate

(b)(6);(b)(7)(C);(b)(7)(F)



Under Secretary Spaulding and DHS personnel visit Hoover dam as part of critical-infrastructure outreach (January 2016). NPPD photo.

The National Protection and Programs Directorate (NPPD)¹ leads the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure. NPPD works closely with partners from all levels of the federal government, and from the private and non-profit sectors to share information and mitigate potential risks from terrorism and natural disasters.

NPPD's workforce is made up of over 3,000 federal employees and 15,000 contractors, including Protective Security Advisors, Chemical Security Inspectors, Federal Law Enforcement Officers, Biometric Identity Services Experts, and field and programmatic support personnel. There are five major components of NPPD:

- Federal Protective Service
- Office of Biometric Identity Management
- Office of Cybersecurity and Communications
- Office of Cyber and Infrastructure Analysis
- Office of Infrastructure Protection

¹ In 2015, the National Protection and Programs Directorate (NPPD) initiated planning to reorganize under functional mission alignments and proposed to change its name to Cyber and Infrastructure Protection.

Federal Protective Service - The Federal Protective Service (FPS) protects federal facilities, their occupants, and visitors by providing law enforcement and protective security services and leveraging intelligence and information resources of federal, state, local, tribal, territorial, and private sector partners.

(b)(6);(b)(7)(C);(b)(7)(F)

The agency's explosive detection canine teams are trained to deploy across the nation and work jointly with other federal, state, and local law enforcement agencies in support of national special security events, emergency situations, and potential threats. NPPD photo.

Office of Biometric Identity Management - The Office of Biometric Identity Management (OBIM) supports the Department of Homeland Security's responsibility to protect the nation by providing accurate and timely biometric identification services across the Homeland Security Enterprise that helps federal, state, and local government decision makers accurately identify the people they encounter and determine whether those people pose a risk to the United States. OBIM matches, stores, shares and analyzes biometric data while protecting the privacy and civil liberties of individuals. OBIM was designated in March 2013 as the lead entity within the Department of Homeland Security for biometric identity management services.

(b)(6);(b)(7)(C);(b)(7)(F)

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 infrastructure in order to protect the public, the economy, and government services. CS&C leads efforts to protect federal executive branch civilian networks and to collaborate with the private sector to increase the security of networks. In addition, the National Cybersecurity and Communications Integration Center (NCCIC) serves as a 24/7 cyber monitoring, incident response, and management center and as a national point of cyber and communications incident integration.

OBIM Biometric Experts provide 24/7 support to identity services. NPPD Photo.

Office of Cyber and Infrastructure Analysis - The Office of Cyber and Infrastructure Analysis' (OCIA) mission is to support efforts to protect the Nation's critical infrastructure through an integrated analytical approach evaluating the potential consequences of disruption from physical or cyber threats and incidents. The results of this analysis will inform decisions to strengthen infrastructure security and resilience, as well as response and recovery efforts during natural, man-made or cyber incidents.

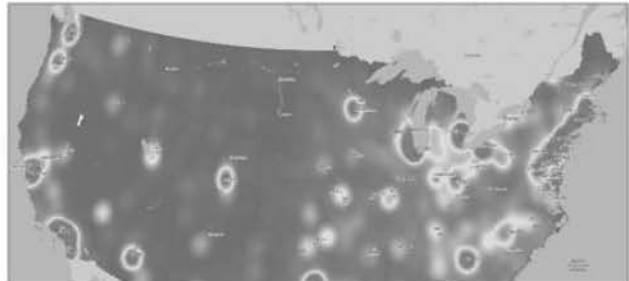
Office of Infrastructure Protection - The Office of Infrastructure Protection (IP) leads and coordinates national programs and policies on critical infrastructure security and resilience and has established strong partnerships across government and the private sector. The office conducts and facilitates 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.

(b)(6);(b)(7)(C);(b)(7)(F)

Protective Security Coordination Division (PSCD) in action. NPPD photo.

Average NPPD Day

- The National Cybersecurity and Communications Integration Center :
 - Receives more than 300 incident reports from Federal, state, and local governments and critical infrastructure
 - Scans 110 Federal agencies, during which scans detect 713 vulnerabilities;
 - Deploys three assessment teams to customer sites and distributes 48 information products such as new vulnerabilities or threat alerts
 - Distributes 253 industrial controls self-assessment tools and trains 42 students in the state-of-the-art industrial controls system lab
- The Federal Protective Service:
 - Provides security for 9,000 General Services Administration-owned or leased federal facilities
 - Protects 1.4 million federal employees and visitors at protected facilities;
 - Prevents 1,760 prohibited items from entering protected facilities
 - Provides oversight for the activities of 13,000 contract Protective Security Officers in the performance of their security duties
- The Office of Cyber and Infrastructure Analysis
 - Meets with critical infrastructure sector stakeholders on the latest analysis of interdependencies and cascading consequences within their sectors
- The Office of Biometric Identity Management
 - Processes 310,280 subjects through the Automated Biometric Identification System (IDENT)



Critical Manufacturing Density Map

OCIA has analysis and geospatial information systems to help decision makers quickly understand and respond to threats and disasters. NPPD product.

- Processes 9,329 watchlist matches through IDENT
- Maintains the IDENT database of more than 200 million unique identities – the largest biometric database in the Federal government
- The Office of Infrastructure Protection
 - Conducts 18 security surveys and assessments to identify vulnerabilities at critical infrastructure
 - Engages with stakeholders at 20 events to provide expert counsel on voluntary protective measures for venues and attendees
 - Provides expertise during the response efforts to three natural or man-made incidents
 - Determines whether four chemical facilities are at high risk of terrorist attack; visits five high-risk facilities to provide security planning assistance, approves six facility security plans, and conducts nine inspections to ensure security measures are accurate and in place
 - Monitors 16 sectors of national critical infrastructure and ensures critical infrastructure situational awareness for DHS leadership
 - Serves as the Sector-Specific Agency for six critical infrastructure sectors

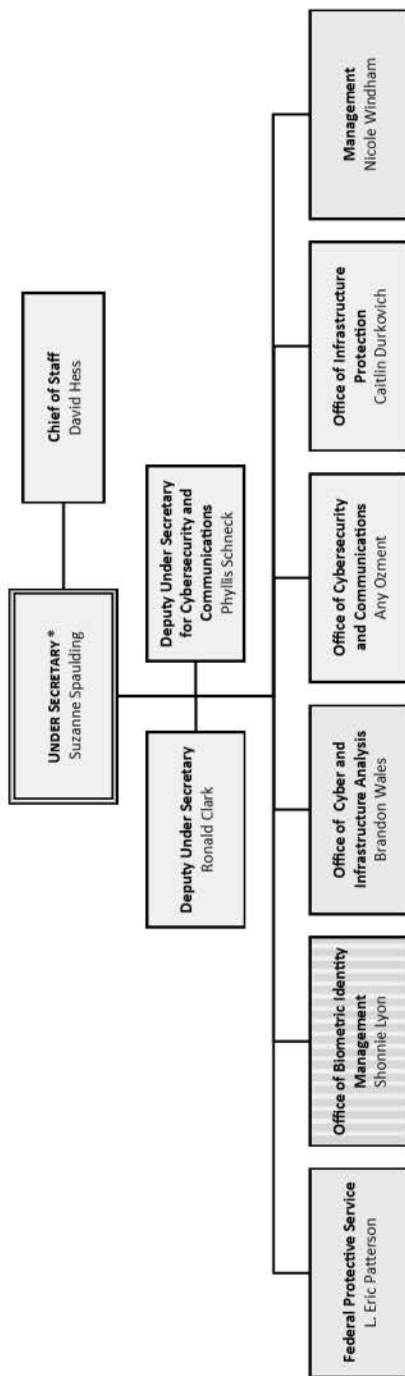
(b)(6);(b)(7)(C);(b)(7)(F)

Mission

NPPD leads the national effort to protect and enhance the resilience of the nation’s physical and cyber infrastructure.

Organization Chart

National Protection and Programs Directorate



Key

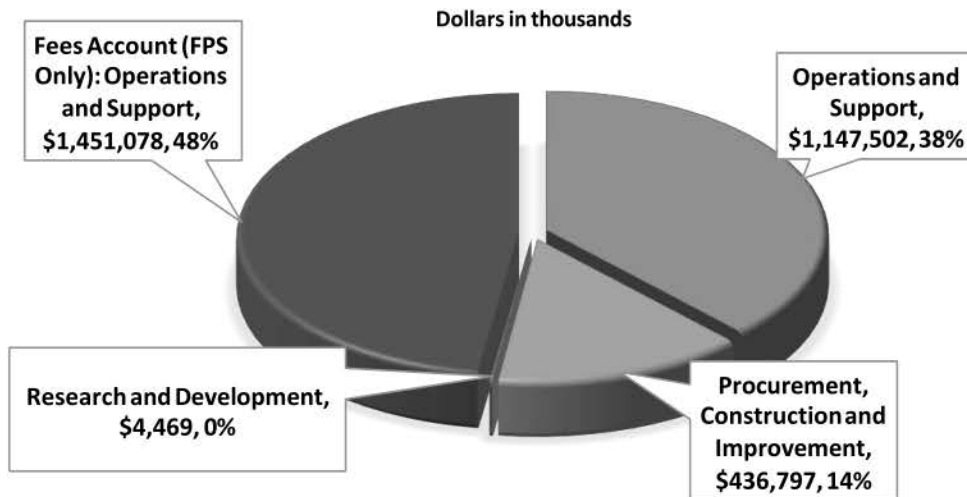
| | |
|-------------------------------|-------------------|
| * Senate Confirmed | ** Reports to OGC |
| Non-Career | Career |
| Acting Non-Career | Acting Career |
| Non-Career or Career Position | |

Warning! This document, along with any attachments, contains NON-PUBLIC INFORMATION exempt from release to the public by federal law. It may contain confidential, legally privileged, proprietary or deliberative process inter-agency/intra-agency material. You are hereby notified that any dissemination, copying, or further distribution of this information to unauthorized individuals (including unauthorized members of the President-elect Transition Team) is strictly prohibited. Unauthorized disclosure or release of this information may result in loss of access to information, and civil and/or criminal fines and penalties.

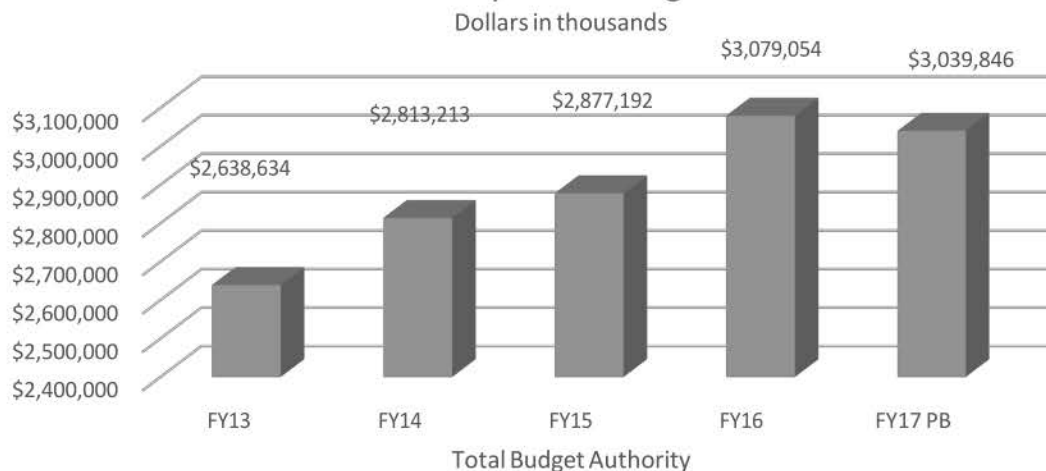
Budget

| NPPD - Total Budget Authority | | |
|-------------------------------|----------------------------|---------------|
| FY 2016 Enacted ² | FY 2017 President's Budget | +/- |
| \$3,079,054,000 | \$ 3,039,846,000 | -\$39,208,000 |

FY17 President's Budget



NPPD - 5-year Funding Trend



² The FY 2016 Enacted Budget places OBIM funding in NPPD and OBIM's budget of \$282,473,000 is reflected in NPPD's total budget authority for FY 2016. The FY 2017 President's Budget Request places OBIM funding under Customs and Border Protection, so the President's Request for OBIM's FY 2017 budget (\$ 305,536,000) is not included in NPPD FY 2017 figures.

Workforce

| Authorized* | Onboard* | Vacancies* |
|-------------|----------|------------|
| 3,782 | 3,145 | 623 |

* FY 2016. Does not include reimbursable, working capital, or revolving account employees

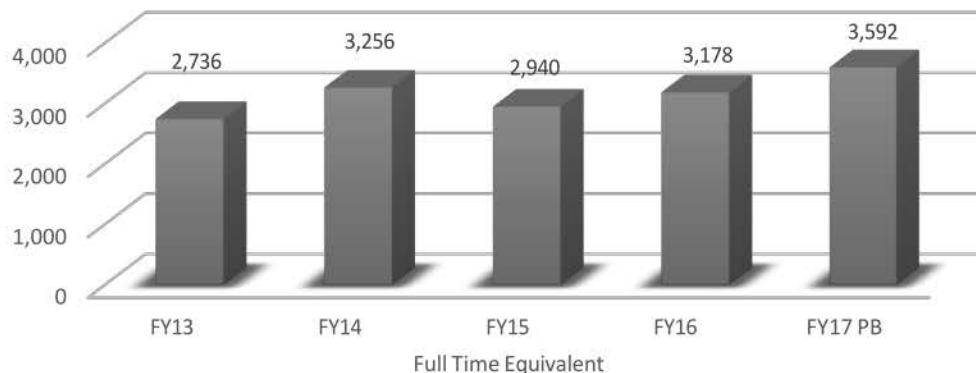
NPPD Workforce Chart

National Protection and Programs Directorate (Totals)
 FTE Authorized: 3782
 FTE Funded: 3178
 FTP Onboard – P (14 current/14 projected)
 FTP Onboard – C (3145 current/3185 projected)
 Vacancy – P (0 current/ 0 projected)
 Vacancy – C (623 current/583 projected)
 Total Vacancy rate (16.5% current/15.4% projected)

| | | |
|---|---|--|
| <p>Federal Protective Service FTE Authorized: (b)(7)(E) FTE Funded: (b)(7)(E) FTP Onboard – P (b)(7)(E) projected) Vacancy – P (b)(7)(E) Vacancy – C (b)(7)(E) Total Vacancy rate (b)(7)(E) projected)</p> | <p>Office of Biometric Identity Management FTE Authorized: 196 FTE Funded: 186 FTP Onboard – P (0 current/0 projected) FTP Onboard – C (153 current/170 projected) Vacancy – P (0 current/0 projected) Vacancy – C (43 current/26 projected) Total Vacancy rate (21.9% current/13.3% projected)</p> | <p>Office of Cyber and Infrastructure Analysis FTE Authorized: 113 FTE Funded: 72 FTP Onboard – P (0 current/0 projected) FTP Onboard – C (79 current/84 projected) Vacancy – P (0 current/0 projected) Vacancy – C (34 current/29 projected) Total Vacancy rate (30.1% current/25.7% projected)</p> |
| <p>Officer of Cybersecurity and Communications FTE Authorized: 922 FTE Funded: 669 FTP Onboard – P (5 current/5 projected) FTP Onboard – C (680 current/656 projected) Vacancy – P (0 current/0 projected) Vacancy – C (237 current/261 projected) Total Vacancy rate (25.7% current/28.3% projected)</p> | <p>Office of Infrastructure Protection FTE Authorized: 761 FTE Funded: 619 FTP Onboard – P (2 current/2 projected) FTP Onboard – C (609 current/600 projected) Vacancy – P (0 current/0 projected) Vacancy – C (150 current/159 projected) Total Vacancy rate (19.7% current/20.9% projected)</p> | <p>Management and Other Mission Support FTE Authorized: 283 FTE Funded: 246 FTP Onboard – P (7 current/7 projected) FTP Onboard – C (204 current/242 projected) Vacancy – P (0 current/0 projected) Vacancy – C (72 current/34 projected) Total Vacancy rate (25.4% current/12% projected)</p> |

Last updated 08/30/2016

NPPD - 5-year Workforce Trend



Warning! This document, along with any attachments, contains NON-PUBLIC INFORMATION exempt from release to the public by federal law. It may contain confidential, legally privileged, proprietary or deliberative process inter-agency/intra-agency material. You are hereby notified that any dissemination, copying, or further distribution of this information to unauthorized individuals (including unauthorized members of the President-elect Transition Team) is strictly prohibited. Unauthorized disclosure or release of this information may result in loss of access to information, and civil and/or criminal fines and penalties.

Strategic Priorities

- Investment Priorities - To address increasing cybersecurity and violent extremist threats in the homeland, NPPD is prioritizing the following investments:

- Acceleration of the availability of the Continuous Diagnostics and Mitigation program and to expand it to encompass new security capabilities;
- Continuing the National Cybersecurity Protection System (EINSTEIN) deployment of new intrusion prevention, information sharing, and analytic capabilities across Federal civilian department and agencies to enhance protection from cyber threats;
- Strengthening partnership and fostering capacity building by increasing the number of Cybersecurity Advisors and Protective Security Advisors in the field;
- Building the Federal Protective Service Rapid Protection Force, which will allow FPS to maintain current protection levels while responding to heightened security threats at specific Federal facilities or geographic areas; and
- Continuing development of the Homeland Advanced Recognition Technology (HART), a DHS-wide mission system to match, store, share, and analyze biometric identity data.

(b)(6);(b)(7)(C);(b)(7)(F)

An FPS Inspector conducts a facility security assessment (FSA) on the technological security measures protecting a federal office building. NPPD photo.

- NPPD Transition – To increase unity of effort and better secure and enhance the resilience of critical infrastructure from cyber and physical threats, NPPD has developed a comprehensive transition plan to reorganize under functional mission alignments. This effort better integrates the organizations and missions that have accumulated within NPPD since its origins as a DHS headquarters component of a few hundred employees to more than 3,000 employees and 15,000 contractors engaged in and supporting operational activity all across the country.



Mobile Command Vehicles (MCVs) can be rapidly dispatched 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. NPPD

- Regional Support Structure - The current risk environment requires operational activity to improve risk management capability at the local level across the country. A more robust regional support structure, as proposed in the NPPD Transition Plan, will strengthen the management, support, and coordination of operational activity to address man-made and natural disasters, as will the Operations Coordination and Watch function proposed for headquarters.

- Situational Awareness and Infrastructure Analysis - NPPD will continue to develop enhanced situational awareness and infrastructure analysis capabilities. This includes onsite assessments following cyber incidents, identification of authoritative data feeds for enhanced situational awareness of critical infrastructure, heightened geospatial analytics, and subject matter expertise to support the Automated Indicator Sharing initiative for “near real time” cyber threat indicator sharing capability.



OCIA modeling, simulation, and analysis helps decision makers understand the likely and ongoing impacts from natural disasters and other threats, which supports response efforts and cuts recovery times. NPPD photo.

- Workforce Development – NPPD needs an integrated capability for recruiting, onboarding, training, and continually developing employees through joint duty or regional assignments. NPPD will continue to develop and implement the Protection Center of Excellence to institutionalize these processes, develop an integrated culture, and enhance mission execution. The Protection Center of Excellence will also provide a center and mechanisms that drive training, knowledge sharing, partnership integration and concept development for the protection professional.

Key Partnerships / Stakeholders

| Interagency | |
|-----------------------------|---|
| Partner | Description |
| Department of Energy (DOE) | This partner is a primary member of the Interagency Security Committee; member of the Critical Manufacturing, Nuclear, and Dams Government Coordinating Councils; houses the Oil and Natural Gas Sector-Specific Agency. |
| Department of Justice (DOJ) | OBIM engages through the Next Generation Identification (NGI) service; For IP, the Federal Bureau of Investigation (FBI) supports coordination and sharing of information during steady-state engagement with private sector partners and incident driven reporting and response; provides intelligence support for risk mitigation and the critical infrastructure protection mission; associate member of the ISC. CS&C works with FBI in ongoing investigations of cyber incidents. |
| Department of State (DOS) | Member of ISC; Member of the Critical Manufacturing and Nuclear Government Coordinating Councils (DHS-SSAs); leads the US delegation to the Global Partnership Against the Spread of Weapons and Materials of Mass Destruction, for which DHS chairs a sub-working group on chemical security; funds programs to promote growth of a global chemical security culture; supports the Office of Bombing Prevention work on PPD-17 and JPO C-IED; supports identification of innovative, cross-sector approaches to enhancing infrastructure resilience with key international partners; OBIM supports the Bureau of Consular Affairs with expanded data matching capabilities, including support to the Visa Waiver Program which contributes to Preventing and Combating Serious Crime to Enforce and Administer Our Immigration Laws. |
| Department of Defense (DoD) | OBIM works with the Defense Forensics and Biometrics Agency on interoperability and data sharing to provide customers and partners with expanded data matching capabilities. CS&C works with DOD in responding to cyber incidents. |

| Interagency | |
|---------------------------------------|--|
| Partner | Description |
| General Services Administration (GSA) | FPS is focused on strengthening its partnership and coordination with GSA by drawing on its shared equities in federal facility security, and in its customer base of federal agencies. In tandem with recent attention the relationship has received from oversight bodies, FPS has embarked on an initiative to work with GSA to better standardize and integrate security practices into federal facility requirements to ensure and implement a rounded and coordinated protective posture for federal facilities. |
| Interagency Security Committee | On October 19, 1995, President Clinton issued Executive Order 12977, creating the ISC to address continuing government-wide security for Federal facilities. Prior to 1995, minimum physical security standards did not exist for nonmilitary Federally owned or leased facilities. Chief security officers and other senior executives from 58 Federal agencies and departments make up the ISC membership. Leadership is provided by the chair, who is the NPPD's Assistant Secretary for Infrastructure Protection, the Program Director, and eight standing subcommittees. |
| Office of Management and Budget (OMB) | CS&C closely coordinates with OMB to administer the Federal Information Security Modernization Act of 2014 and Binding Operational Directives. For IP, as a collaborative, membership-based organization, interagency involvement is key to the mission of the ISC. This partner is a primary member of the ISC, as outlined in E.O. 12977. |

| Stakeholder Groups and Federal Advisory Committees (FACA) | |
|--|--|
| Partner | Description |
| Critical Infrastructure Partnership Advisory Council (CIPAC) | Government Coordinating Council and Sector Coordinating Council members for all 16 sectors |
| National Infrastructure Advisory Committee (NIAC) | <p>The NIAC was created by Executive Order 13231 of October 16, 2001 and continued by a series of Executive Orders. The Council is composed of not more than 30 members, appointed by the President, who are selected from the private sector, academia, and State and local government, representing senior executive leadership expertise from the critical infrastructure critical infrastructure sectors as delineated in Presidential Policy Directive 21.</p> <p>The NIAC provides the President, through the Secretary of Homeland Security, with advice on the security and resilience of critical infrastructure, both physical and cyber, supporting sectors of the economy</p> |
| National Security Telecommunications Advisory Committee (NSTAC) | <p>The NSTAC is composed of up to 30 Presidentially-appointed senior executives who represent various elements of the telecommunications industry. The committee advises the President on a wide range of policy and technical issues related to telecommunications, information systems, information assurance, infrastructure protection, and other national security and emergency preparedness (NS/EP) concerns. The NSTAC meets quarterly via conference calls and in-person meetings to report its activities while providing recommendations to the President.</p> <p>The NSTAC was established by Executive Order 12382 in September 1982 to advise the President on matters regarding NS/EP telecommunications. DHS is the Executive Agent for the NSTAC.</p> |

| Industry / Public-Private / Academia | |
|--|--|
| Partner Name | Description |
| National Association of Security Companies (NASCO) | FPS coordination with NASCO facilitates the agency's national implementation of security standards across its contracted Protective Security Officer workforce. FPS's close working relationship with the organization facilitates transparent dialogue to support centralized communication with its vendors and vast PSO workforce, and to standardize security standards and operations across its portfolio of federal facilities. |

| International Engagements | |
|-----------------------------------|---|
| Partner | Description |
| The Five Country Conference (FCC) | The FCC is a consortium of government immigration agencies from Australia, Canada, New Zealand, United Kingdom, and the United States of America. International data sharing to Enforce and Administer Our Immigration Laws. (OBIM) |

| Organized Labor / Advocacy Groups | |
|--|--|
| Partner | Description |
| American Federation of Government Employees (AFGE) Local 918 | AFGE Local 918 represents certain employees in NPPD within FPS and IP. |

(b)(5)

***Government Accountability Office / Office of the Inspector General
Audits***

| GAO Audits | | | |
|--|----------------------|--|---|
| Title | Report Number | Description | Final Report Due |
| Review of DHS's National Cybersecurity and Communications Integration Center (NCCIC) | 100533 | National Cybersecurity Protection Act of 2014 and the Cybersecurity Act of 2015 require GAO to review aspects of NCCIC including whether: (1) the NCCIC aligns with requirements set forth in both laws and (2) if NCCIC is effectively fulfilling requirements to support its cybersecurity mission. | December 2016 |
| Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress | Report No. 16-79 | GAO began this work pursuant to its authority under 31 U.S.C. 717 after receiving a request from Ranking Member Bennie Thompson of the House Committee on Homeland Security. Report includes seven recommendations, two of which are directed to DHS. | Published: Nov 19, 2015. Publicly Released: Nov 19, 2015 |
| Critical Infrastructure Protection: DHS and State Need to Improve Their Process for Identifying Foreign Assets and Systems | Report No. 15-223C | GAO began this work pursuant to its authority under 31 U.S.C. 717 after receiving a request from Ranking Member Bennie Thompson of the House Committee on Homeland Security. GAO's report included three recommendations, which are all still considered open at this time | Report is FOUO, therefore not released to the public. __ |

| GAO Audits | | | |
|--|----------------------|--|---|
| Title | Report Number | Description | Final Report Due |
| Homeland Security: FPS and GSA Should Strengthen Collaboration to Enhance Facility Security | Report No. 16-135 | GAO began this work pursuant to its authority under 31 U.S.C. 717 after receiving a request from Ranking Member Bennie Thompson of the House Committee on Homeland Security. There are a total of eight recommendations to this report, four for DHS, and the other four for GSA. All eight recommendations are open at this time. | Published: Dec 16, 2015. Publicly Released: Jan 15, 2016 |
| Federal Protective Service: Enhancements to Performance Measures and Data Quality Processes Could Improve Human Capital Planning | Report No. 16-384 | GAO is began this work in response to a congressional mandate (S. Rpt. 113-198 To Accompany P.L.114-4, the Department of Homeland Security Appropriations Act of 2015. Title III - Protection, Preparedness, Response, and Recovery. Federal Protective Service) There are three recommendations to this report, and they are all open at this time. | Published: Mar 24, 2016. Publicly Released: Mar 24, 2016 |

DHS Transition Issue Papers

Secure Handling of Ammonium Nitrate (AN) Act

BACKGROUND:

In 2007, Congress passed a statute adding provisions to the Homeland Security Act directing DHS to promulgate a rule by December 2008 for regulating, at the point of sale, transactions involving ammonium nitrate (AN) to include

- Registration and vetting against the Terrorist Screening Database of all purchasers and sellers of ammonium nitrate products.
- Verification of registered/vetted status at the point-of-sale.
- Recordkeeping requirements and DHS inspections of records.
- Requirements to report thefts/losses of ammonium nitrate.

CHALLENGES TO IMPLEMENTING THE STATUTE:

Although DHS has been developing a draft final rule, it has not finalized the rule and published it in the Federal Register. The currently envisioned Ammonium Nitrate regulation would be very expensive to implement and would impose significant burdens upon the public. The costs and burdens would greatly outweigh any security benefits that would be attained. While implementation of a final rule could mitigate some of the terrorism risk associated specifically with ammonium nitrate, it would by no means cover all AN transactions. Moreover, the statute presents a single-chemical solution for what, in the Department's view, is a multiple-chemical IED precursor threat as identified in the following figure. To the extent the statute might succeed incrementally in deterring attacks involving AN, it could merely shift the risk to the many other IED precursor chemicals for which a point-of-sale regulatory framework would not be in place.

(b)(5)



RECOMMENDED PATH FORWARD

(b)(5)



Warning! This document, along with any attachments, contains NON-PUBLIC INFORMATION exempt from release to the public by federal law. It may contain confidential, legally privileged, proprietary or deliberative process inter-agency/intra-agency material. You are hereby notified that any dissemination, copying, or further distribution of this information to unauthorized individuals (including unauthorized members of the President elect Transition Team) is strictly prohibited. Unauthorized disclosure or release of this information may result in loss of access to information, and civil and/or criminal fines and penalties.

DHS Transition Issue Papers

(b)(5)

Warning! This document, along with any attachments, contains NON-PUBLIC INFORMATION exempt from release to the public by federal law. It may contain confidential, legally privileged, proprietary or deliberative process inter-agency/intra-agency material. You are hereby notified that any dissemination, copying, or further distribution of this information to unauthorized individuals (including unauthorized members of the President elect Transition Team) is strictly prohibited. Unauthorized disclosure or release of this information may result in loss of access to information, and civil and/or criminal fines and penalties.

The National Protection and Programs Directorate's Regional Footprint Now and In The Future

The National Protection and Programs Directorate (NPPD) has a Federal workforce of more than 3,000 employees and 13,000 contracted Protective Security Officers stationed across the country and in the territories.

- NPPD leverages a cadre of 301 staff to provide technical assistance in the field, supporting both voluntary and regulatory critical infrastructure protection and resilience programs. These staff include Protective Security Advisors, Cyber Security Advisors, Chemical Security Inspectors, and Office of Emergency Communications Regional Staff.
- NPPD additionally has 1,282 Federal Protective Service (FPS) staff responsible for mitigating risks to Federal facilities and enforcing Federal and state laws in locations nationwide
- Regional Cybersecurity and Communications staff are located in Pensacola, Florida and Idaho Falls, Idaho.

NPPD is in the process of expanding its regional staff, shifting previously headquarters-based programs, such as administrative support functions and training and exercises, into the field to enable more efficient service delivery to stakeholders and support region-specific mitigation efforts.

OFFICE OF INFRASTRUCTURE PROTECTION

NPPD's Office of Infrastructure Protection's (IP) regionalization planning effort began in FY 2015, with initial implementation activities commencing in FY 2016. The 10 regions align with the commonly used federal regions. NPPD has leveraged opportunities in the majority of regions to collocate with Federal Emergency Management Agency (FEMA) or other federal partners to maximize cost savings. IP's Regional Enhancement Plan is currently undergoing internal review.

Regional Locations:

| Region Number | Metropolitan Area in which IP Regional Office will be Located |
|---------------|---|
| I | Boston, MA |
| II | New York, NY |
| III | Philadelphia, PA |
| IV | Atlanta, GA |
| V | Chicago, IL |
| VI | Dallas, TX |
| VII | Kansas City, MO |
| VIII | Denver, CO |

| | |
|----|----------------|
| IX | Menlo Park, CA |
| X | Seattle, WA |

IP secured approval to hire Regional Directors and initial support staff. The 10 Regional Directors serve as the senior officials in each region and are accountable for the execution of the IP field operations support services; coordinating efforts between IP and Office of Cybersecurity and Communications (CS&C) personnel in the field; executing the voluntary technical assistance and outreach mission (i.e., non-regulatory) in the region; working with the IP regulatory mission; and developing and executing a regional strategy.

FEDERAL PROTECTIVE SERVICE

NPPD’s FPS protects Federal facilities and their occupants, including more than 1200 law enforcement officers based in 250 distinct locations throughout the United States and the territories of Guam and Puerto Rico.

- FPS field operations are primarily conducted through a Region/District/Area organization.
 - There are 11 FPS regions (see map below), each of which are led by a GS-15 Regional Director. FPS Regions largely align geographically with FEMA Regions. Due to the concentration of federal facilities within the NCR, FPS has a Region 11 which covers the NCR.
 - Each Region is subdivided into three-four Districts, which are led by GS-14 District Commanders. There are 37 FPS Districts nationwide.
 - Each District is subdivided into Areas based upon the geographic workload. Areas are led by GS-13 Area Commanders.
- FPS has three Assistant Directors of Field Operations (ADFO), who are members of the Senior Executive Service and who are based in the field. They provide primary operational oversight to Regional Directors.
- FPS has four dispatch and communications MegaCenters. These centers – located in Michigan, Colorado, Pennsylvania, and Maryland – are in operation 24 hours a day, 7 days a week. They serve as Public Safety Answering Points for the federal community, Emergency Communications Centers for FPS law enforcement operations, monitor stations for multiple types of alarm systems, and wireless dispatch communications centers throughout the nation.
- Each Region has an incident command vehicle capability allowing region leadership to rapidly deploy to an event and establish command and control of deploying elements.
- FPS established an initial Rapid Protection Force (RPF) capable of responding to threats or disasters to provide critical protection related activities. Establish internally with existing resources in September of 2015, dedicated resources are requested in the FY2017 President’s Budget.



CYBERSECURITY AND COMMUNICATIONS

NPPD’s Cybersecurity and Communications (CS&C) mission continues to grow to keep pace with increasingly sophisticated and persistent cybersecurity threats and evolving risks such as the Internet of Things. In addition to its Headquarters staff, CS&C field facilities and staff are located in Idaho Falls, Idaho, Corry Station in Pensacola, Florida. CS&C also maintains a nascent presence in Silicon Valley, California.

- The facility in Idaho Falls supports the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), an operational arm of the National Cybersecurity and Communications Integration Center (NCCIC). The Idaho facility has a fully functional watch floor along with unclassified space in several buildings.

- The facility in Corry Station supports engineering, data analysis, and management functions for the National Cybersecurity Protection System, more commonly known as EINSTEIN. The Corry Station facility also has a fully functional watch floor and analytic capabilities to conduct forensic analysis of cybersecurity threats.
- CS&C has assigned a representative to open a small office in Silicon Valley, California for purposes of industry outreach.
- CS&C also has Regional Field staff assigned through the country, including Cyber Security Advisors and Emergency Communication Regional Coordinators. These employees are included in and will be supported by the Regional Enhancement Plan described above.

OFFICE OF BIOMETRIC IDENTITY MANAGEMENT (OBIM)

NPPD's Office of Biometric Identity Management (OBIM) is the designated lead entity within DHS responsible for providing biometric identity services. OBIM delivers these services to DHS and its mission partners through the Automated Biometric Identification System (IDENT), which stores over 200 million unique biometric identities of individuals who have applied for admission to the United States, have applied for visas and immigration benefits, have applied for DHS credentialing services, or have significant derogatory information associated with them (e.g., wanted persons, suspected terrorists). OBIM's capacity to match, store, share, and analyze biometric data, provides decision makers on the front lines of homeland security with rapid, accurate, and secure identity services that help keep our country safe from those who wish to do our nation harm. OBIM's Biometric Support Center (BSC) is an integral part of IDENT's biometric identity capability and meets this mission critical need by providing 24/7, expert biometric identity services.

- As more stakeholders realize the value of biometrics and the benefit of searching the over 200 million identities contained in IDENT, demand for OBIM's biometric identity management services continues to grow from both within the Department and from external stakeholders resulting in increased demand for BSC services. NPPD is assessing the need for BSC regional offices to support regional partners.
- OBIM Federal personnel currently reside in four locations: Arlington, Virginia; DHS Data Center, Clarksville, Virginia; DHS Data Center, Stennis, Mississippi; and the Biometric Support Center West, San Diego, California.

RFI 183 Overview of Cyber Authorities

a. What does DHS have?

The Department's cyber responsibilities, including information sharing, technical assistance, protection of federal civilian networks, and cyber incident response are specifically authorized in the Homeland Security Act (HSA or Act), as amended. The National Cybersecurity Protection Act of 2014 amended the Act to establish DHS's National Cybersecurity and Communications Integration Center as the federal-civilian interface for "shared situational awareness to enable real-time, integrated, and operational actions across the Federal Government and non-Federal entities." 6 U.S.C. § 148(c)(2). The Act broadly authorizes the National Cybersecurity and Communications Integration Center to provide "technical assistance, risk management support, and incident response capabilities to federal and non-federal government entities with respect to cyber threat indicators, defensive measures, cybersecurity risks, and incidents, which may include attribution, mitigation, and remediation" which authorizes the National Cybersecurity and Communications Integration Center's "fly-away" teams. 6 U.S.C. § 148(c)(6). For significant cyber incidents, Presidential Policy Directive – 41 designated DHS, through the National Cybersecurity and Communications Integration Center, as the lead Federal agency for asset response.

The Federal Information Security Modernization Act of 2014 requires DHS to administer the implementation of information security policies and practices for federal, executive branch, civilian agencies. Among other activities, the Federal Information Security Modernization Act of 2014 authorizes DHS to assist the Office and Management and Budget in its Federal Information Security Modernization Act of 2014 duties, to monitor implementation of agency information security policies and practices, to deploy technology to assist agencies to continuously diagnose and mitigate against cyber threats and vulnerabilities, and to develop and oversee the implementation of information-security-related binding operational directives to other agencies. Provisions in the Cybersecurity Act of 2015 require DHS to deploy technical capabilities – i.e., EINSTEIN – to detect and prevent cybersecurity risks in the network traffic of federal agencies, and require agencies to apply EINSTEIN. The Federal Information Security Modernization Act of 2014 also places in DHS the federal information security incident center, a role DHS fills with the United States Computer Emergency Readiness Team.

To support the Department's broad mission to lead the national effort to enhance the security resilience, and reliability of the Nation's cyber and communications infrastructure through NPPD, the Secretary has a range of workforce authorities which are exercised through the Office of the Undersecretary for Management. The Department also has authority to investigate crimes and administer programs contributing to the nation's general cybersecurity through the U.S. Secret Service, Immigration and Customs Enforcement, and the U.S. Coast Guard.

- Consistent with the Cybersecurity Workforce Assessment Act, section 3 of the Border Patrol Agent Pay Reform Act of 2014, and the Homeland Security Workforce Assessment Act, the Secretary has authority to assess the cybersecurity workforce of the Department, develop and

~~Warning! This document, along with any attachments, contains NON-PUBLIC INFORMATION exempt from release to the public by federal law. It may contain confidential, legally privileged, proprietary or deliberative process inter-agency/intra-agency material. You are hereby notified that any dissemination, copying, or further distribution of this information to unauthorized individuals (including unauthorized members of the President-elect Transition Team) is strictly prohibited. Unauthorized disclosure or release of this information may result in loss of access to information, and civil and/or criminal fines and penalties.~~

implement a new excepted service human capital personnel system, and develop additional recruitment and retention incentives.

- Consistent with 18 U.S.C. § 3056(a), the Secret Service assesses and mitigates cybersecurity risks to systems that could impact the agency's protective mission. The Secret Service also has explicit authority to investigate access-device and computer fraud offenses. For example, the Secret Service investigates cyber crimes that have a significant economic or community impact, involve organized criminal groups or international organizations, or involve novel misuses of information technology.
- The USA PATRIOT Act of 2001 (Pub.L 107-56, Sec. 105, 18 U.S.C. § 3056 note) requires the Secret Service "to develop a national network of electronic crime task forces, based on the New York Electronic Crimes Task Force model, throughout the United States, for the purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems."
- Immigration and Customs Enforcement's Homeland Security Investigation Special Agents, as Immigration and Customs Criminal Investigators, investigate violations of criminal laws found in Titles 8, 18, 19, 21, 22, 31, 46 and 50 of the U.S. Code, including situations in which computers are used in the commission of those crimes, the digital theft of intellectual property and export controlled data. When charges or potential charges are being considered pursuant to a criminal investigation, Homeland Security Investigations will, as appropriate, include violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.
- The Human Exploitation Rescue Operations Act of 2015 amends the Homeland Security Act and directs the Department to operate, within Homeland Security Investigations, a Cyber Crimes Center to provide investigative assistance, training and equipment to support domestic and international investigations by Homeland Security Investigations of cyber-related crimes. 6 U.S.C. § 473(a). The law also codifies Homeland Security Investigations' specific cybercrime and cybersecurity authorities by creating a Cyber Crimes Unit within the Cyber Crimes Center, which oversees the cyber security strategy and cyber related operations and programs for Homeland Security Investigations. 6 U.S.C. § 143(d).
- The U.S. Coast Guard serves as the Sector Specific Agency (as defined by the National Infrastructure Protection Plan) for the Maritime Transportation Subsector (delegated by DHS). The Coast Guard has certain authorities over regulated facilities and vessels. Through the Captain of the Port and Officer in Charge, Marine Inspection, the Coast Guard is working to integrate cyber threats into its regulatory regime.

b. What are the gaps? (include resource information)

In general, Congress has provided DHS with broad authorities to carry out its mission and needs appropriations commensurate with these authorities.

c. What does DHS need?

DHS needs an amendment to the Homeland Security Act of 2002 to allow DHS administrative subpoena power. The National Cybersecurity and Communications Integration Center does not have subpoena power and must engage law enforcement partners to issue a subpoena to an Internet Service Provider (ISP) for the identity of the owner of an affected Internet Protocol address to inform them of a possible system compromise or increased risk of cyber intrusion.

Warning! This document, along with any attachments, contains NON-PUBLIC INFORMATION exempt from release to the public by federal law. It may contain confidential, legally privileged, proprietary or deliberative process inter-agency/intra-agency material. You are hereby notified that any dissemination, copying, or further distribution of this information to unauthorized individuals (including unauthorized members of the President-elect Transition Team) is strictly prohibited. Unauthorized disclosure or release of this information may result in loss of access to information, and civil and/or criminal fines and penalties.

This is especially important to NPPD's responsibilities in asset response under Presidential Policy Directive 41 "United States Cyber Incident Coordination." Organic subpoena power would allow the National Cybersecurity and Communications Center to obtain information through an administrative rather than law enforcement process, shorten the response time, enhance the National Cybersecurity and Communications Integration Center's ability to carry out its existing statutory functions, and help minimize damages from a cyber intrusion.

Additionally, DHS continues to support update to law enforcement provisions related to cybersecurity, a national data breach notification standard, and updates to improve law enforcement ability to recover digital evidence. As examples, see the January 13, 2015 proposals, (available at: https://www.whitehouse.gov/omb/legislative_letters), and the July 15, 2016 proposal on "Permitting the Secure and Privacy-Protective Exchange of Electronic Data for the Purposes of Combatting Crime Including Terrorism."

d. What can incoming leadership do to help fix?

- DHS has proposed legislation, which has cleared the interagency process and OMB, clarifying NPPD's operational status. The proposed legislation would also change NPPD's name to the Cyber and Infrastructure Protection Agency. Continued Departmental support in seeking enactment of this legislation will greatly enhance NPPD's ability to accomplish its mission in this space.
- Presently non-federal entities report incidents to the Department on a voluntary basis. Mandatory data breach notification to victims and/or the Department is a policy proposal for consideration.
- Cybersecurity continues to be an active policy area for legislative proposals in Congress. Working with Congressional committees to ensure that legislative proposals do not conflict with current authorities continues to be an important focus.

| Activity | Title/Description | Associated PR # | Estimated Award Date | Expected Period of Performance |
|----------|--|----------------------|----------------------|--------------------------------|
| FPS | PSO Services- FPS Region11 | *HSHQEC-16-R-00004 | (b)(5) | |
| FPS | PSO Services- FPS Region11 | 192117R11GRDP0104 | | |
| FPS | PSO Services- FPS Region11 | 192116PELGRDS701 | | |
| FPS | PSO Services- FPS Region11 | 192116PELGRDS094 | | |
| FPS | PSO Services- FPS Region11 | 192117R11GRDP0900 | | |
| FPS | PSO Services- FPS Region11 | 192117R11GRDP0102 | | |
| FPS | Personnel Security Services (NOTE: OASIS PROCUREMENT) | 192116PHQPSDP1055 | | |
| FPS | PSO Services- FPS Region 3 (Philly Metro) | 192116PTHPLP0185 | | |
| FPS | Land Mobile Radio Refresh (NOTE: DHS Strategic Sourcing Vehicle TACCOM IDIQ) | 192116PHQCMDP0017 | | |
| FPS | PSO Services – FPS Region 6 (IA, KS, MO & NE) | 192116R060000P115 | | |
| FPS | Instructor services at FLETX in support of FPS TPD | 192175DD000P0016 | | |
| FPS | PSO Services for Northern California (HSHQW9-16-R-00002) | 192116PNINC17001 | | |
| FPS | PSO Services for Central California (HSHQC7-16-R-00003) | 192116PNICC17001P000 | | |
| FPS | PSO Services for Western WA (HSHQWA-16-R-00002) | 192116PTE4020P9032 | | |
| FPS | PSO Services for Southern WA and Oregon (HSHQWA-17-R- 00001) | 192116PTE4020P9031 | | |
| FPS | Region 7 Administrative Support Services (HSHQC7-17-R-00002) | 192117R07RCNP0181 | | |
| FPS | CCV and IDS Install in Los Angeles, CA (HSHQW9-17-Q- 00006) | 192117R09CP05P109 | | |
| NPPD | Multi-Modal Examiners | RNIM-17-00004 | | |
| NPPD | Standing Desk | RNIM-17-00005 | | |
| NPPD | Priority Services Scientific Engineering, Technical, and Assistance Support Services | RNCC-17-50002 | | |
| NPPD | CS&C Front Office Technical Assessments and Studies | RNCC-17-60007 | | |
| NPPD | Glass and Wood Award Trophies | RNUS-17-0001 | | |
| NPPD | Facility Rental (Minneapolis, MN) | RNCC-17-30003 | | |

Massachusetts Institute of Technology
Lincoln Laboratory

**Evaluation of the
Department of Homeland Security
National Cybersecurity Protection System**

(b)(6)

Technical Report EIN02

7 December 2015

Transmittal inside MIT Lincoln Laboratory must have prior approval of the Lincoln Laboratory Program Manager.

No secondary distribution is authorized without prior written approval of the appropriate U.S. Government controlling agency.

Lexington

Massachusetts

Table of Contents

| | |
|---|-----------|
| 1. EXECUTIVE SUMMARY | 3 |
| 1.1. INTRODUCTION..... | 3 |
| 1.2. MAIN FINDINGS..... | 3 |
| 1.3. RECOMMENDATIONS..... | 5 |
| 2. INTRODUCTION | 8 |
| 3. E³A BACKGROUND | 10 |
| 3.1. E ³ A OVERVIEW AND DESIGN GOALS..... | 10 |
| 3.2. E ³ A CURRENT STATUS AND CAPABILITIES..... | 11 |
| 3.3. E ³ A USE AT GOVERNMENT DEPARTMENTS AND AGENCIES (D/As)..... | 14 |
| 3.4. FEEDBACK AND E ³ A FEATURE REQUESTS FROM D/AS | 14 |
| 3.5. RECENT GOVERNMENT BREACHES..... | 16 |
| 3.6. INFORMATION SHARING WITH NCPS-IS..... | 18 |
| 4. MAJOR FINDINGS | 21 |
| 4.1. PERIMETER DEFENSE ALONE IS NO LONGER EFFECTIVE AGAINST ADVANCED PERSISTENT THREATS (APTs)..... | 21 |
| 4.2. E ³ A BLACKLISTS ARE BENEFICIAL BUT ARE UNLIKELY TO PREVENT THE MOST ADVANCED THREATS | 22 |
| 4.3. WE HAVE NOT SEEN EVIDENCE THAT THE BENEFIT OF CLASSIFIED E ³ A INDICATORS JUSTIFIES THEIR COST..... | 24 |
| 4.4. E ³ A DOES TOO LITTLE TO HELP D/AS RAPIDLY DETECT AND DISRUPT BREACHES | 25 |
| 4.5. E ³ A IS NOT INTEGRATED WITH CDM AND OTHER D/A SECURITY TOOLS AND PROCEDURES..... | 26 |
| 4.6. USE OF NCPS-IS IS TOO LABOR INTENSIVE AND IT IS NOT INTEGRATED WITH E ³ A AND CDM | 27 |
| 4.7. WE SAW LITTLE EVIDENCE TO INDICATE THAT DHS IS USING ITS GLOBAL VIEW OF THE CYBERSECURITY STATE OF THE D/AS TO MAXIMUM ADVANTAGE..... | 27 |
| 5. RECOMMENDATIONS | 29 |
| 5.1. UNTIL THE VALUE OF CLASSIFIED E ³ A SIGNATURES IS DEMONSTRATED, WITHHOLD INVESTMENT IN FURTHER EXPANSION OF NCPS SECURITY SERVICES..... | 29 |
| 5.2. FOCUS ON ENABLING DEPARTMENTS AND AGENCIES TO RAPIDLY RESOLVE ALERTS AND DISRUPT BREACHES | 30 |
| 5.3. BEFORE EXPANDING OR MANDATING E ³ A ACROSS D/AS, CREATE A HIGH-LEVEL SECURITY ARCHITECTURE | 31 |
| 5.3.1. SYSTEMS ENGINEERING PROCESS..... | 32 |
| 5.3.2. AN EXAMPLE NCPS HIGH-LEVEL ARCHITECTURE | 34 |
| 5.4. DETERMINE HOW TO BEST TAKE ADVANTAGE OF THE UNIQUE DHS CENTRALIZED VIEWPOINT .. | 35 |
| 5.5. ENABLE TIMELY DISSEMINATION OF NCPS-IS INFORMATION TO D/AS AND ENSURE IT BENEFITS D/A SECURITY WORKFLOWS..... | 36 |

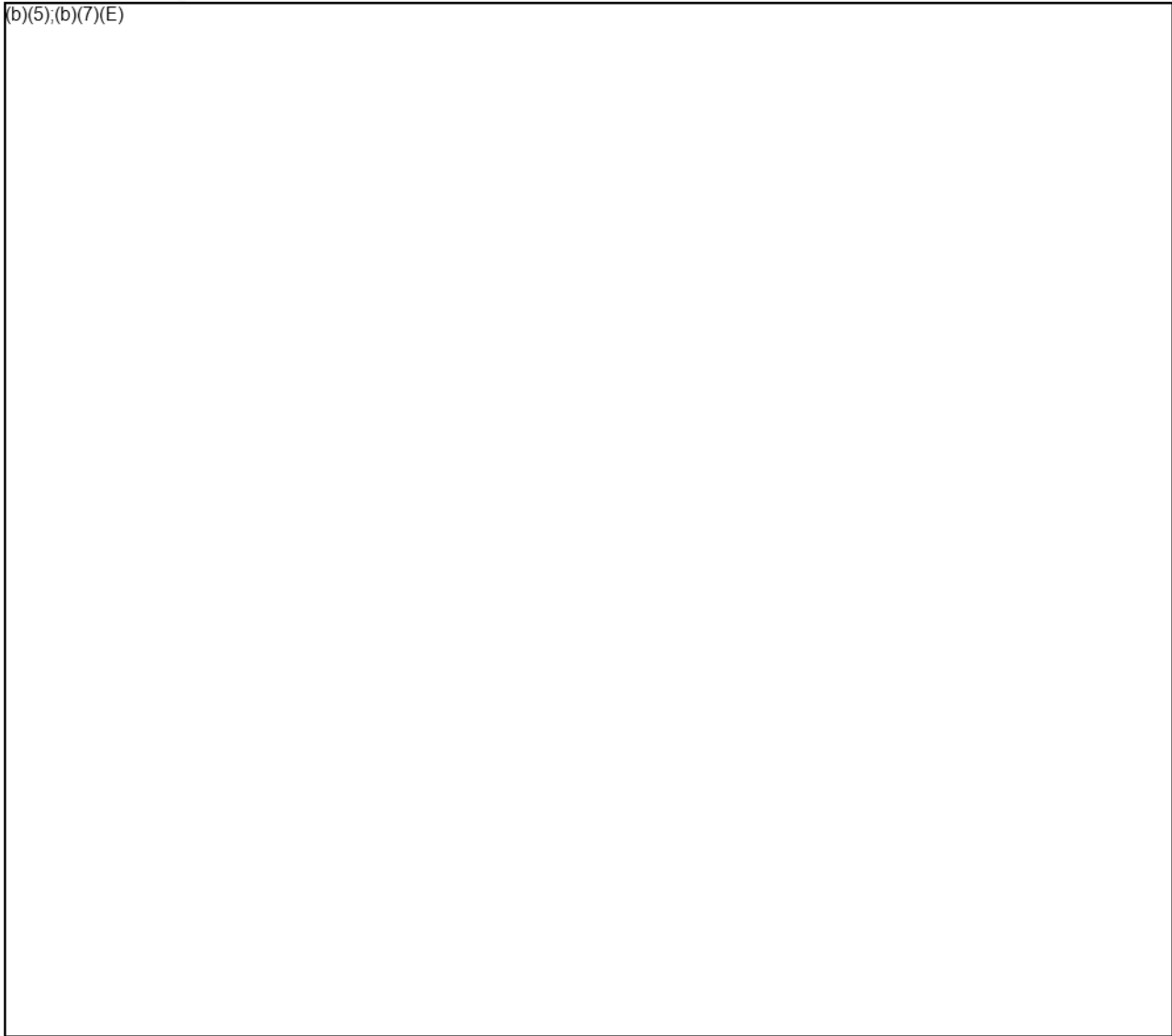
1. Executive Summary

1.1. Introduction

This report describes an independent evaluation performed by MIT Lincoln Laboratory of several of the main components of the National Cybersecurity Protection System (NCPS) developed and managed by the Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD). This evaluation started in March 2015 focusing on the EINSTEIN 3 Accelerated (E³A) intrusion protection system and the NCPS Information Sharing (NCPS-IS) architecture. The initial scope was expanded to include more general recommendations on securing government Departments and Agencies (D/As) following the announcement in June 2015 of a major breach at the Office of Personnel Management (OPM).

1.2. Main Findings

(b)(5),(b)(7)(E)



2. Introduction

This report describes an independent evaluation performed by MIT Lincoln Laboratory of several of the main components of the National Cybersecurity Protection System (NCPS) developed and managed by the Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD). This evaluation started in March 2015 focusing on the EINSTEIN 3 Accelerated, E³A, intrusion protection system and the NCPS Information Sharing architecture. The initial scope was expanded to include more general recommendations on securing government Departments and Agencies (D/As) following the announcement in June 2015 of a major breach at the Office of Personnel Management (OPM). The timeline of this report is shown in Figure 1.

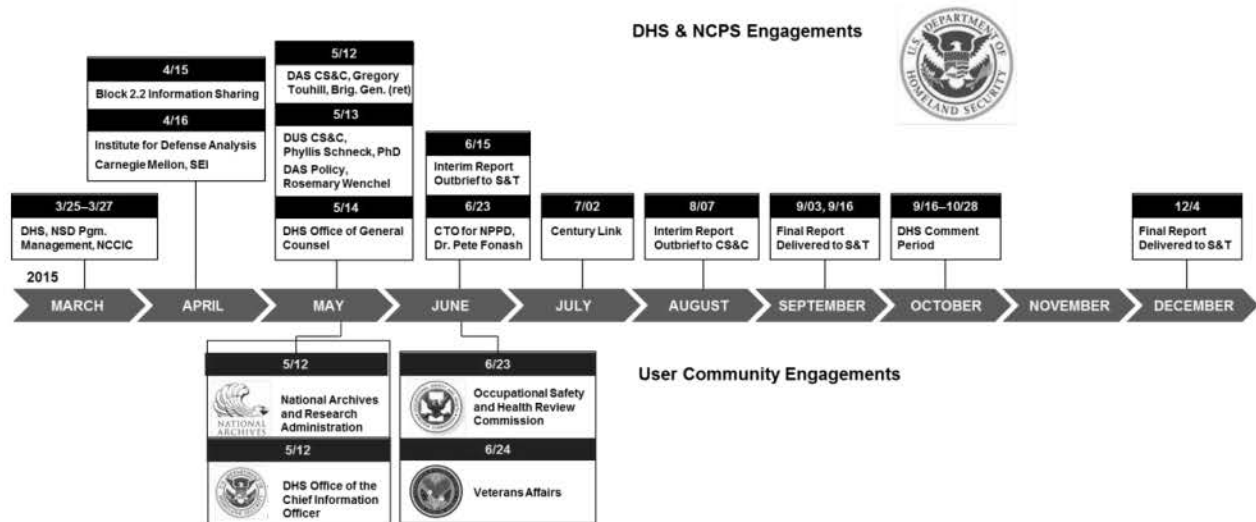


Figure 1. Timeline for Lincoln study of NCPS

The National Cyber Protection System has been developed to protect the information systems of the civilian U.S. Government from intrusion and attack, especially from foreign cyber threats. DHS is tasked with improving cyber security for more than 100 civilian government departments and agencies ranging in size from 10's to 100's of employees (such as the Selective Service System) to more than 250,000 employees (such as the Department of Veterans Affairs). DHS has no direct authority over these agencies and needs to honor the privacy of citizens who trust government D/As with their private and personal information. DHS roles described in the Comprehensive National Cybersecurity Initiative (CNCI) released in January 2011 include deploying an intrusion detection system called EINSTEIN 2 to monitor traffic to and from D/As, deploying an intrusion prevention system called EINSTEIN 3 (now called E³A) to block attacks to D/As, and coordinating and integrating cyber information to provide situational awareness across D/As. In addition a DHS program called Continuous Diagnostics and Mitigation (CDM) provides tools and services that strengthen the security posture of D/As through continuous monitoring and corrective actions.

This report focuses on the E³A intrusion prevention component of the EINSTEIN program and its

effectiveness in protecting government D/As. We were also asked to analyze the information sharing elements of NCPS (NCPS-IS) and have done so. The findings and recommendations provided below are based on interviews with DHS personnel and contractors, on interviews with four D/A Chief Information Security Officers (CISOs) and other Federal and DoD Government partners, on E³A and CDM documentation, and on openly available information on DHS, CDM, D/As, recent breaches, threats, and the effectiveness of different types of defenses.

(b)(7)(E)



3. E³A Background

3.1. E³A Overview and Design Goals

In 2008, the Department of Homeland Security envisioned a perimeter based Intrusion Prevention System called EINSTEIN 3 that would protect the cyber assets of U.S. civilian Government networks. The system built on earlier phases of the EINSTEIN program, which placed sensors and analytic capabilities at Trusted Internet Connections (TICs). In addition to protecting government D/As, a major goal of the system was to obtain visibility across D/As that contributes to national intelligence situational awareness. This IPS program was subjected to several directed changes in technical approach. E3A evolved into its current form from EINSTEIN 3 with its approval for acquisition in April 2012.

Early assumptions and design decisions had a major effect on the current structure and effectiveness of E³A. Some of these early assumptions were as follows:

1. A perimeter, signature-based system is a necessary part of a defense-in-depth strategy.
2. Classified indicators are required to maximize value.
3. Countering sophisticated threat actors requires advanced countermeasures that must be deployed within the ISP infrastructure.
4. The commercial market is mature enough to offer solutions that can evolve with changing threats/technologies.
5. The impact on D/As must be minimized.

Some of these assumptions were based upon legal and policy mandates. They were not backed by a strong technical justification when the program began, have not yet been proven or evaluated, but they have been retained even through the evolution of EINSTEIN 3 into E³A. For example, no careful analysis has demonstrated the advantage of classified indicators, even though they significantly contribute to the cost and complexity of the program. No careful analysis demonstrated that a perimeter signature based system would be most beneficial for D/As. In fact, most D/As currently have many controls including perimeter defense that examines many more traffic types than are examined by E³A and they might be better served by assistance in detecting and disrupting breaches. Finally, no analysis has demonstrated that best protection is provided while minimizing the integration impact on D/As. In fact, our discussions with D/As suggest that a better approach might have been to determine the major weaknesses of D/A controls and design E³A specifically to address those weaknesses.

The E³A program has a long and rather complex history, but the first ISP contract was awarded in 2013. In this report we describe the system as observed in April-May 2015. It should be noted the E³A system is rapidly changing, especially following the Office of Personnel Management (OPM) breach that was made public in June 2015. Some of the details we provide, such as the number of D/As using E³A are changing daily, but the overall design goals, the assumptions, and the design decisions listed above remain the same.

3.3. E³A Use at Government Departments and Agencies (D/As)

The current E³A program is being rapidly expanded following the OPM breach announced in June 2015. The Secretary of Homeland Security Jeh Charles Johnson announced on 8 July 2015 that E³A currently protects 931,000 federal personnel, or approximately 45% of the federal civilian government¹ and that plans are to make E³A available to all D/As by the end of 2015. This is a dramatic increase in coverage compared to the roughly 15% we observed a few months earlier.

Although the coverage is larger now, we assume that usage of E³A components has remained similar. Seven D/As with more than 500 employees were using E³A services when this study was performed. (b)(7)(E)

(b)(7)(E)

We assume that as E³A usage expands, the main service being used is DNS redirection. This service is relatively easy to use and has little impact on a D/A. We assume that fewer D/As will take advantage of E³A email filtering. This is possibly because D/As see the service as redundant because they already provide their own email filtering as indicated by the 2014 FISMA report². It could also be related to the difficulty of setting up E³A email filtering and the potential for greater disruption if E³A fails.

3.4. Feedback and E³A Feature Requests from D/As

We interviewed the four D/As shown in Table 1 concerning desired features for E³A, the current protection provided, and performance compared with their own internal controls. These include three D/As of different sizes that were using E³A at the time of this study, one small D/A (OSHRC) that was

(b)(7)(E)

¹Remarks by Secretary of Homeland Security Jeh Charles Johnson on “Securing The.Gov” 8 July 2015, <http://www.dhs.gov/news/2015/07/08/remarks-secretary-homeland-security-jeh-charles-johnson-securing-gov>

²Annual Report to Congress: Federal Information Security Management Act, Office of Management and Budget, 27 Feb 2015 as retrieved from https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf

| Name | Acronym | Employees ³ (www.allgov.com) | (b)(7)(E) |
|--|---------|--|-----------|
| Department of Veterans Affairs | VA | 250,000 | |
| Department of Homeland Security ⁵ | DHS | 208,000 | |
| National Archives and Records Administration | NARA | 1,660 | |
| Occupational Safety and Health Review Commission | OSHRC | 65 | |

Table 1. Characteristics of four D/As interviewed concerning E³A.

(b)(7)(E)

³ This table reference the number of US Government employees, DHS figures reference employees plus contractors.

⁴ As of 9/9/2015, Lincoln was informed that Veterans Affairs has subscribed to E³A email filtering

⁵ Note that since the interview with DHS Office of the CIO on 12 May 2015 that DHS has subscribed to E³A services.

(b)(7)(E)



3.5. Recent Government Breaches

The Office of Personnel Management (OPM) announced one of the most devastating breaches of a U.S. government agency on 4 June 2015⁷. Data stolen included sensitive information for 21.5 million individuals contained in background investigation databases. Personal information stolen included financial histories, social security numbers, children's and relatives' names, foreign contacts, and residences. Such information could benefit foreign intelligence agencies, support highly tailored spear-phishing attacks, and lead to theft of credentials that are created or verified using detailed personal information.

The OPM breach announced in June 2015 was not an isolated incident, but the fourth breach by attackers into OPM background investigation databases that has occurred over the past 12 months. Two of these breaches were directly into OPM and two were into OPM contractors holding background investigation data. The upper part of Figure 4 shows the four public breaches for OPM from the past year in chronological order with some details for each breach. This figure was created using data from the Privacy Rights Clearinghouse⁸. OPM breaches were announced in July 2014, August 2014, December

⁶ The Heartbleed Bug, 2 Sept 2015, <http://heartbleed.com/>

⁷ <https://www.opm.gov/cybersecurity/>

⁸ <http://www.privacyrights.org/data-breach>

2014, and June 2015. In the last three breaches, the number of personal records stolen increased from 25,000 to 40,000 to 21,500,000. The second and third attacks were against contractors employed by OPM. The former OPM director, Katherine Archuleta, explained in congressional testimony reported in the *Federal Times*⁹ that attackers obtained credentials from an OPM contractor named “Keypoint” in the third 2014 breach and then used them in the most recent massive breach to obtain access to the main OPM database as shown by the dotted line in Figure 4. It was relatively easy to use the stolen credentials because OPM did not require two-factor authentication to remotely access their systems. Database encryption would not have helped in this breach because attackers used valid credentials and could access OPM data at will.

None of the EINSTEIN program components provided indication of the four OPM breaches when they first occurred because they were new attacks and signatures were not available in EINSTEIN¹⁰. The most recent and most serious breach was discovered when DHS and other agencies helped OPM improve its internal network detection and monitoring tools in early 2015, partly as a response to the three preceding breaches. OPM receives EINSTEIN 2 IDS services through its Trusted Internet Connections but does not subscribe to E³A IPS services. New internal analysis tools discovered new malicious activity in April 2015. Indicators and the resulting signatures developed as part of this analysis were then added to the EINSTEIN intrusion detection component, which discovered that the attack was an ongoing breach of OPM’s systems and the Department of Interior data center it used. These signatures were then used by EINSTEIN to search for similar attacks across other D/As. Note that reports suggest the breach began in December 2014 and that it was not detected until four months later in April 2015. EINSTEIN 2 helped in a post mortem analysis of the breach and once the breach was understood and helped find other instances of the same attack, but it didn’t help detect the initial attack.

⁹ <http://www.federaltimes.com/story/government/omr/opm-cyber-report/2015/06/23/keypoint-isis-opm-breach/28977277/>

¹⁰ <http://arstechnica.com/security/2015/06/why-the-biggest-government-hack-ever-got-past-opm-dhs-and-nsa/>

A Chronology for Breaches of U.S. Government Agencies

July 2014 to June 2015

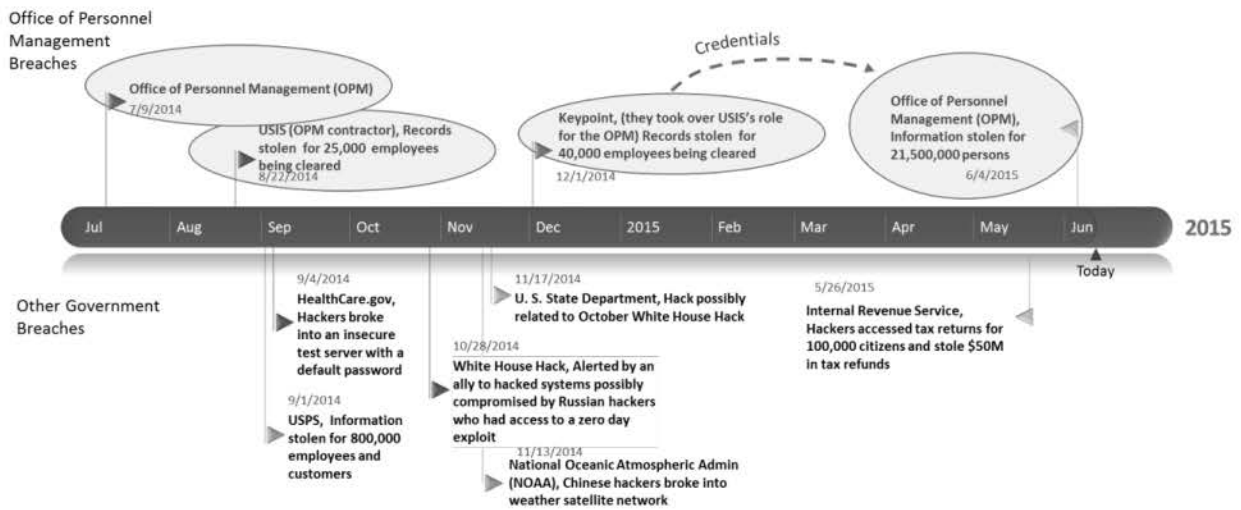


Figure 4. A Chronology of Breaches of U.S. Government Agencies July 2014 to June 2015¹¹

The lower part of Figure 4 provides the date and details for six other breaches from the past year distributed across many government agencies. For the May 2015 IRS breach, attackers first used PII information (Social Security number, date of birth, address and tax filing status) to access past returns and then used the information they gained from these old returns to file fraudulent returns. Before they were stopped, attackers accessed tax returns for 100,000 citizens and stole \$50M in tax refunds. The U.S. State Department and White House breaches appeared to be related and associated with Russian attackers who had access to zero-day attacks that could not be detected by signature-based systems. The NOAA attack provided attackers access to websites used to provide weather information to the public including forecasts for airlines and other transportation companies. The USPS breach appears to have been carried out by a sophisticated actor who did not appear to be interested in identity theft or credit card fraud, but only in capturing detailed information on USPS employees. E³A was not in a position to detect any of the six breaches in the lower part of Figure 4. We can presume that the attacks in the figure that used stolen or known credentials would not have been found by the current E3A because of the lack of capability to examine anything except for email and DNS queries.

3.6. Information Sharing with NCPS-IS

The *National Strategy to Secure Cyberspace*, Presidential Policy Directive 21 (PPD 21), and other executive orders charge DHS with the role of ensuring collaboration amongst the larger cyber community to detect, respond, and learn about cyber threats, and to help the cyber community provide context to attacks and prioritize protection. In the event of an attack, DHS must also coordinate response between

¹¹ Chart derived from data at <http://www.privacyrights.org/data-breach>

multiple entities and provide situational awareness to key participants. The purpose of the National Cybersecurity Protection System Information Sharing (NCPS-IS) initiative is to develop, deploy, and maintain a set of information sharing capabilities to enable shared situational awareness, collaboration, and coordination across multiple participants. These participants are multiple and include Federal civilian Departments and Agencies (D/As); Foreign Partners; State, Local, and Tribal Governments; private sector partners; and critical infrastructure owners. Key goals of NCPS-IS are to improve the efficiency of existing participant processes, reduce their response time to incidents, and enable mutually beneficial cyberspace defenses that leverage each participant's unique skills and perspective.

While still in the early stages of acquisition, NCPS-IS is planned to have nine capabilities. Three components are considered user facing and consist of an information-sharing portal, document and content management, and collaboration. The remaining six capabilities, considered infrastructure enabling consist of content discovery, identity, credentials and access management (ICAM), automated data exchange, cross domain solution, information flow monitoring, and interoperability. The infrastructure enabling capabilities are well considered and appropriate to similar information sharing activities around the Federal government.

The relationships are unclear between the planned NCPS-IS, the legacy cyber information sharing programs such as FLARE and Data Management System, and the evolving Automated Indicator Sharing efforts between Homeland Security and the private sector. In addition, DHS already operates an information-sharing portal called the Homeland Security Information Network (HSIN). While the HSIN is not specifically about cyber information it does have unclassified capabilities that are similar to four of the six NCPS-IS infrastructure enabling, and two of the user-facing capabilities. It is a topic for further study as to how many of these efforts could be replaced by a single framework.

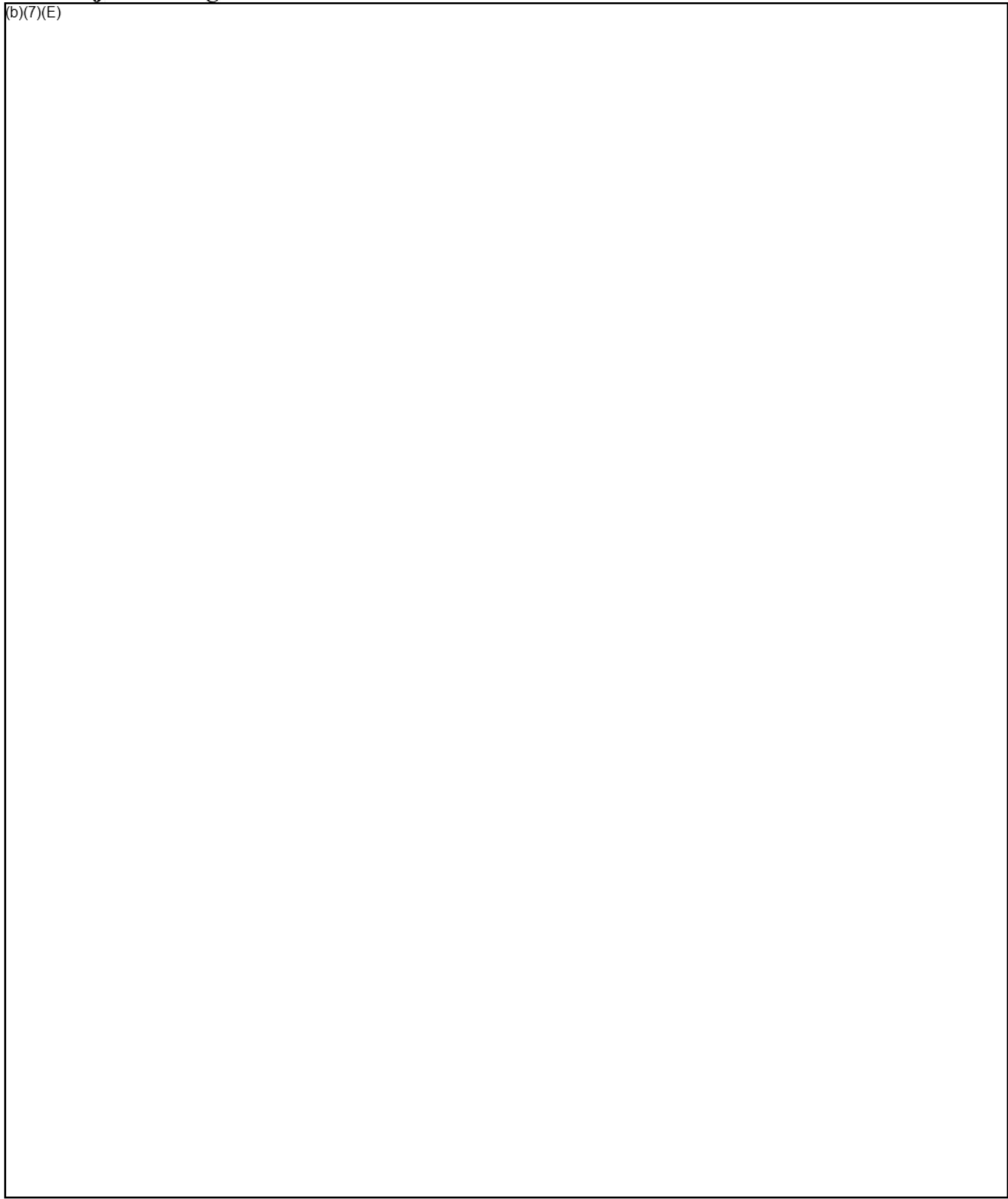
Regarding the cyber-specific information-sharing capability for automated data exchange, NCPS-IS is planned to leverage other Executive Branch information sharing efforts such as those fostered under ESSA to develop an Enhanced Shared Situational Awareness (ESSA) Information Sharing Architecture (ISA) for use by the U.S. Government. The automated data exchange capability currently focuses on cyber indicator sharing and collaboration, but does not currently address other types of cyber information sharing such as courses of action and mitigations. NCPS-IS is planned to be the primary mechanism to feed indicators to E³A. There are plans to make appropriate subsets of information available to the D/As.

The infrastructure for information sharing is a good start at increasing the responsiveness of the cyber defense of Government systems. We do have concerns that the plans do not go far enough in automating the complete life cycle of the use of cyber information. The processes that follow the dissemination of indicators— generation of signatures, testing and validation, dissemination and deployment of final signatures, and deprecation when no longer useful all appear to be personnel intensive. Complete automation of this process is essential to having a cyber defense system that is responsive to the current threat. Furthermore, given that DHS will have knowledge of the security tools deployed internal to the D/As through the CDM program it is possible for DHS to speed the bolstering of the internal defenses by pre-processing indicators into a usable form that need only be validated by the individual D/As before

deployment.

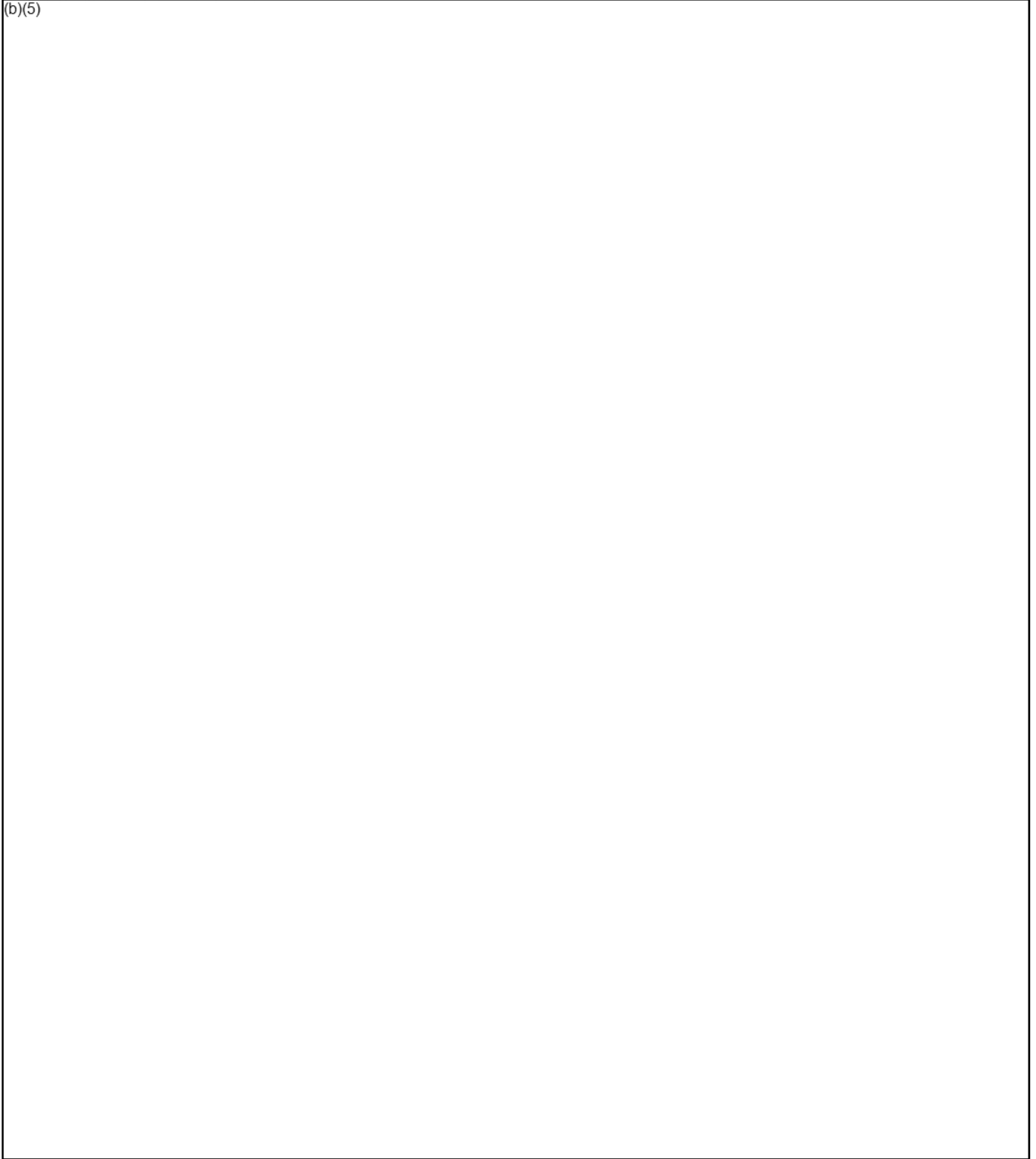
4. Major Findings

(b)(7)(E)



5. Recommendations

(b)(5)



DHS Response to Recent Evaluations of the National Cybersecurity Protection System

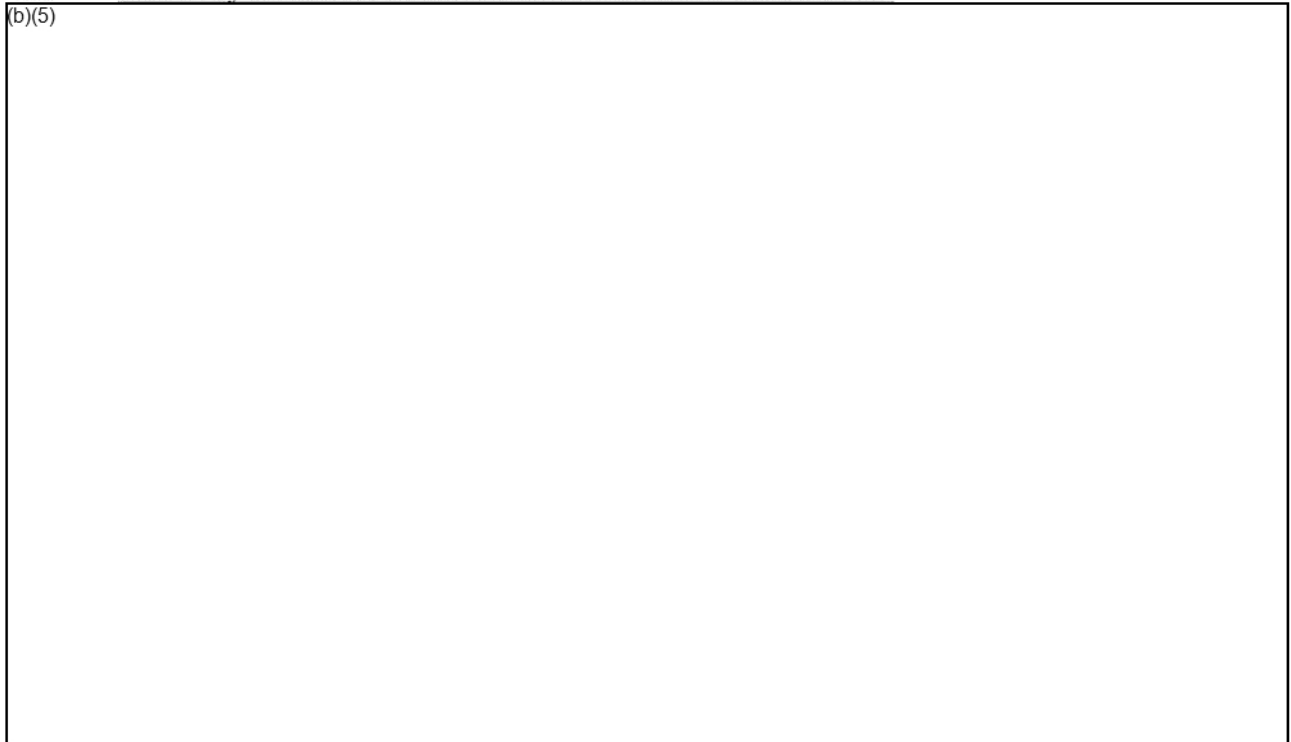
I. Overview:

In the interest of ensuring that federal civilian networks are effectively protected from cyber threats, DHS continually assesses its major cybersecurity programs. These assessments are conducted both internally and by soliciting input from experts outside of government. To this end, DHS recently commissioned two studies: one by the Massachusetts Institute of Technology (MIT) Lincoln Labs and one by a group of government, academic, and private sector experts. This second group was entitled the “Blue Ribbon Panel.” Both groups assessed the National Cybersecurity Protection System, a part of which is the EINSTEIN program, and the Continuous Diagnostics and Mitigation (CDM) program. However, MIT Lincoln Labs had more time to analyze the substance and nuances of both programs. The Blue Ribbon Panel had limited time to conduct its analysis, less experience in how the U.S. government manages major acquisitions, and less understanding of the DHS role in federal cybersecurity. Independent of the MIT Lincoln Labs and “Blue Ribbon Panel” evaluations, the Government Accountability Office recently concluded an assessment of the National Cybersecurity Protection System.

The final reports from all three groups include many recommendations for improvement and DHS will actively seek to address those areas. There are also areas where DHS is operating under externally imposed restrictions, such as Intelligence Community requirements to protect classified information or legal limitations based upon current DHS authorities. Some of the recommendations, therefore, fundamentally misunderstand how the federal government is structured and funded, and minimal likelihood of significant changes therein. Accordingly, DHS does not embrace all of the recommendations.

II. Summary of Recommendations and Associated DHS Actions:

(b)(5)




(b)(5);(b)(7)(E)

How DHS Is Addressing Recommendations:

Warning! This document, along with any attachments, contains NON-PUBLIC INFORMATION exempt from release to the public by federal law. It may contain confidential, legally privileged, proprietary or deliberative process inter-agency/intra-agency material. You are hereby notified that any dissemination, copying, or further distribution of this information to unauthorized individuals (including unauthorized members of the President-elect Transition Team) is strictly prohibited. Unauthorized disclosure or release of this information may result in loss of access to information, and civil and/or criminal fines and penalties.

(b)(5);(b)(7)(E)

(b)(5);(b)(7)(E)



(b)(5);(b)(7)(E)

Finally, we must recognize that in order to remain effective, the E3A program must be able to evolve at the pace of the cyber adversary. Because we are part of the federal government, there are rules and restrictions in place that often create a set of bureaucratic procedures that affect the speed by which a program such as E3A can evolve. There are practices and solutions to overcome these challenges, but the program must have ready and ongoing access to these avenues.

While architectural changes are required to ensure E3A remains relevant, affordable, and effective, we must not lose sight of the fact that this program now allows DHS to not only detect malicious activity across the federal, civilian, executive branch, but actively defend against it. While currently restricted to just e-mail and DNS, those remain the two most active threat vectors used by our adversaries to gain access to and/or compromise .gov networks. DHS continues to understand the great responsibility of providing enterprise cybersecurity services to the .gov enterprise. Although significant strides have been made over the history of the program to deliver on our objectives to provide situational awareness and be a first line of defense against our cyber adversaries, more must be done. DHS must continually assess deficiencies in our architecture, governance models, and technical and management approaches and move at the speed of the threats to make continuous improvements, both strategic and incremental, in each area.



QUICK FACTS

- To fund its services, FPS relies entirely on security charges paid by the federal agencies it protects.
- Basic Security Charge: \$0.78 per square foot
- Building-Specific Oversight Charge: 8%
- Agency-Specific Oversight Charge: 8%

CONTACT FPS

- FPS Mega Center:
1 (877) 437-7411
- FPS Public Affairs:
(202) 732-8055

Security Charges

The Federal Protective Service is responsible for protecting more than 9,000 federal facilities and for safeguarding the millions of employees, contractors, and visitors who pass through those facilities every day. From screening visitors to investigating suspicious packages, FPS delivers comprehensive physical security and law enforcement services to federal agencies residing in spaces leased or owned by the General Services Administration.

Protective Services for Federal Agencies

FPS works with its “tenant customers” – federal agencies in GSA facilities – to conduct security assessments and design countermeasures to mitigate risks. FPS also oversees contract protective security officers, performs criminal investigations, monitors security alarms, and provides many more services to federal agencies. While customers may not use the entire range of FPS services every day, FPS provides peace of mind that they are always protected and can be called upon on a moment’s notice.

Security is not a one-size-fits-all solution. Not every building is the same, and every agency faces different risks. FPS recognizes the diversity across federal facilities, and works with its customers to tailor a solution to meet their security needs. Additionally, FPS always seeks to improve security services for its federal customers, and communicates regularly with the agencies it protects.

Security Charges

FPS does not receive congressional appropriations. To fund its operations, employees, and services to its customers, FPS relies entirely on offsetting collections for all expenses it incurs. FPS recovers the cost of the security it provides via monthly security charges, which are paid by the federal agencies it protects. Federal agencies set aside a portion of their annual budget to pay for security charges, based on an FPS cost estimate of what security services will cost that year. FPS recovers those costs by charging agencies in monthly increments via the DHS monthly security bill.

FPS revenue comes from three categories of security charges:

- **Basic Security Charge:** protection services, risk mitigation, and threat management
- **Building-Specific Charges:** countermeasures benefiting all building occupants
- **Agency-Specific Charges:** countermeasures benefiting an individual agency



Basic Security Charge

The basic security charge pays for services such as facility security assessments, risk management, preliminary investigations, the detention of suspects, 24-hour security alarm monitoring, response to emergency calls, and awareness training for employees.

This fee is charged to all federal agencies occupying a GSA-controlled space. Each tenant is charged based on the square footage it occupies. Currently, the basic security fee is \$0.78 per square foot.

Building-Specific Security Charge

The building-specific security charge pays for the unique security requirements of a specific facility. This includes the contract protective security officers who provide visitor screening, access control, and patrolling. This also pays for the purchase and maintenance of technical countermeasures, such as x-ray machines and camera systems.

This fee is charged to all tenants in a building. Since the benefits are shared, the cost of building security is jointly funded by tenants based on the percentage of space they occupy within the building. Tenants are charged the estimated direct costs of these building-specific services, plus an oversight fee of 8 percent of the overall cost to cover oversight and overhead costs.

Agency-Specific Security Charge

Often times, individual federal agencies request additional security services to meet specific mission needs. For example, an agency may want card readers with intrusion detection systems, or an agency-specific protective security officer.

If an agency desires security measures beyond what FPS has recommended as part of its facility security assessment, that federal agency must submit a Security Work Authorization form and negotiate an agreement with FPS. Agencies are charged the estimated direct cost of these security services, plus an oversight fee of 8 percent of the overall cost to cover the oversight and overhead costs.

Changes to Charging Rates

The U.S. Office of Management and Budget sets the rates for FPS security services annually. OMB will approve any changes to security rates, and will notify agencies in its annual budget guidance. FPS also distributes an annual rate letter to agency Chief Financial Officers.

The Federal Protective Service is a component of the National Protection and Programs Directorate.



The National Protection and Programs Directorate

Agency Landing Team December 15, 2016

NPPD Strategic Overview

DHS Vision: With honor and integrity, we will safeguard the American people, our homeland, and our values. NPPD Vision: A safe, secure, and resilient infrastructure where the American way of life can thrive. NPPD Mission: Lead the national effort to secure and enhance the resilience of the Nation's infrastructure.

| Strategic Objective Provide Situational Awareness | Strategic Objective Reduce Risk | Strategic Objective Protect Infrastructure |
|--|---|--|
| <p>Core Functions Develop, Analyze, and Disseminate Information Incident Reporting, Open Source, Field Reports/Assessments Modeling and Simulation.gov Monitoring Dynamic Prioritization of Infrastructure Risk Analysis Consequence Analysis Share Information across Government and Private Sector Data Integration and Visualization Information Exchange on Threats and Hazards Automated Indicator Sharing</p> | <p>Core Functions Partnership and Capacity Building Work with critical infrastructure owners and operators in the field and at the national level to identify and reduce vulnerabilities Guide National unity of effort for critical infrastructure security and resilience Training on active shooter, CIED, mass casualty, cyber incidents Interoperable Communications guidance and training Assessments Vulnerability Assessments Federal Facility Assessments</p> | <p>Core Functions Security and Law Enforcement Services Protect Government Assets, Systems, and Networks (physical, virtual, and human) Federal Network Security Regulate highest risk chemical facilities Incident Management and Response Cybersecurity Response Physical Incident Response Analytic Support/Response</p> |

Current Events

- Inauguration security planningEnhanced federal protection operations including Operation Blue Surge and operations in Charleston, South Carolina and San Juan, Puerto Rico, and at Dakota Access Pipeline demonstrationsHolidays and Special Events (e.g. NYC Marathon, Macy's Thanksgiving Day Parade, etc.)Election systems security effort

Significant Ongoing Activities

Focus on supporting our highest-priority customers: Ongoing targeted cybersecurity assessment and protection of federal High-Value Assets
Prioritize risk management assistance to critical infrastructure where a cyber attack could have catastrophic impacts
Complete Joint U.S-Canada Strategy for Electric Grid Security
Finalize the National Cyber Incident Response Plan
Advance cybersecurity collaboration with international allies and promote global norms
Address an evolving terrorist threat: Soft target security/Active Shooter training (malls, stadiums, federal agencies)
Bombing prevention and counter improvised explosive devices efforts
Expand biometric identity services to incorporate all of the DOD records, cover all TSA & Chief Security Officer populations, and international information sharing agreements

Additional Areas of Focus

- **Address emerging cybersecurity risks**
Aviation Cybersecurity Initiative
Position, Navigation, and Timing
Advance federal cybersecurity through EINSTEIN and Continuous Diagnostics and Mitigation
Expand operational capability to protect critical infrastructure
Establishing Protection Center of Excellence
Work to secure infrastructure against Non-Traditional Aviation Threats
Continued buildout of the Rapid Protection Force
Re-tiering of Chemical Facility Anti-Terrorism Standards facilities based on revised risk assessment

Leadership Perspective: Concerns/Challenges

- “What keeps your component head awake at night?” Homegrown violent extremists/lone actors
Complex, mass attacks
Cyber event with cascading physical impacts
Significant breach of Federal systems
Nation-State attack on critical infrastructure

Maximizing the resources we have is essential to advancing the mission. Failure to fully integrate relationships, capabilities, information, resources, etc. could have a significant impact.

Leadership Perspective: Concerns/Challenges

- What immediate problems do you need the new Administration's help/support to resolve?
Legislative authority for organizational agility
Expanding Protective Security Officer response authorities
Positioning, Navigation, and Timing - Administration's Support
Sustain focus on compliance with Cybersecurity Binding Operational Directives
Maintain DHS cyber mission space
Implementation of Cyber Authorities – filling vacancies and keeping momentum
Federal contracting provisions for cybersecurity
Resolving Ammonium Nitrate regulatory stalemate
Information sharing initiatives related to increased use of biometrics as a common attribute

Leadership Perspective: Budget Priorities

- What are the top budget priorities for NPPD? Supporting key programs in the Budget Continuous Diagnostics and Mitigation NCCIC Staff Homeland Advanced Recognition Technology Field capacity

Leadership Perspective: Opportunities

- Finalize unity of effort
Significantly enhance cyber resources and capabilities
Better execute authorities in statute
Evolution of identity and the critical role biometric plays

Closing

- DHS has significantly advanced in cybersecurity capacity and capability over the past decade. There is more work to do – our adversaries are increasing in sophistication. Success requires an integrated focus on cyber, physical, and human components of risk and mitigation. Cannot succeed without full understanding of the business of critical infrastructure and true private-public collaboration, made possible by unique legal authorities, and long-developed relationships. With continued focus and the ongoing support of Congress, we will continue to reduce the likelihood and consequence of a cybersecurity incident affecting the infrastructure and services on which we all depend.

Back-up

National Protection and Programs Directorate

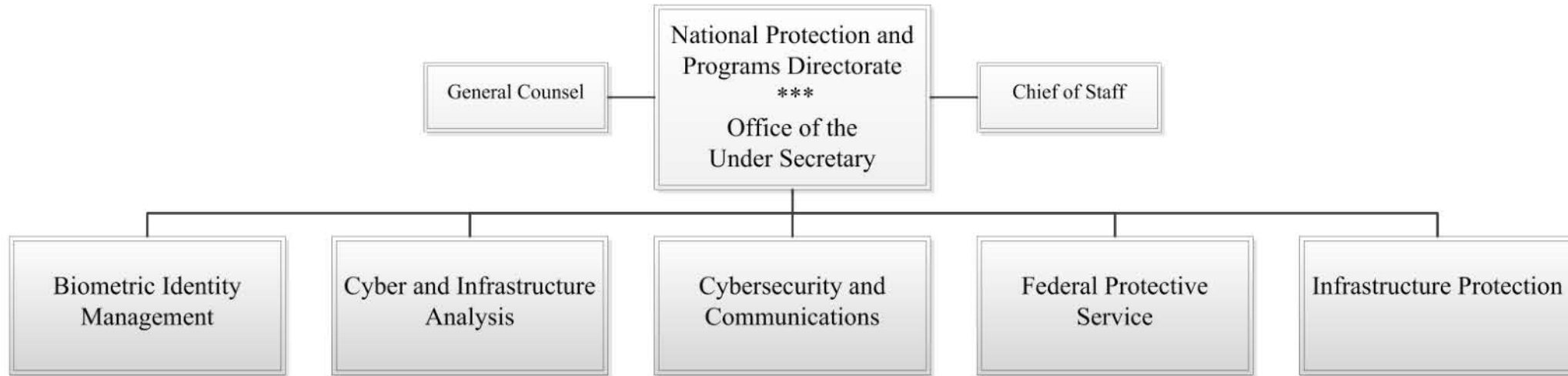
- Our mission is to protect cyber and critical infrastructure Terrorism and other physical threats Growing cyber threats Our work provides a holistic risk management approach for 16 sectors, asset-focused and system- and network-focused, with unique legal authorities supporting true private public collaboration We build cyber and physical risk management capacity of federal partners, private sector owners and operators, state and local agencies, and others



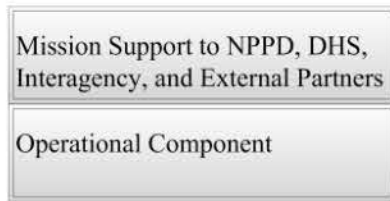
Risk-Based Approach to Cyber and Infrastructure Protection

- Assess and prioritize risks by understanding: Threats (cyber and physical) Vulnerabilities Consequences Work with our partners to develop strategies and capabilities to mitigate across all three through IT and non-IT measures

Organizational Overview



Key:



Mission Evolution

- We have grown from 500 employees to more than 3,000 employees and 15,000 contractors (including more than 13,500 Protective Security Officers) engaging in and supporting operational activity all across the country We have engaged in an in-depth evaluation of both our structure and our business model: We are now an operational entity with wide-ranging responsibilities for ensuring the security and resilience of the Nation's infrastructure against physical and cyber threats To ensure we have the agility required to be successful, the Congress is considering proposals to change NPPD's name to Cyber and Infrastructure Protection and to empower us with flexibility to make some internal organizational improvements We are making changes to emphasize and support operational activities, particularly in the field