Cyber and Infrastructure Protection Transition Way Ahead

Fiscal Year 2016 Report to Congress

March 17, 2016

Homeland Security

Executive Summary

In October 2015, DHS provided Congress a plan to transition the National Protection and Programs Directorate (NPPD) to an organizational structure that would address the growing risks to critical infrastructure. This current report provides additional details about why and how this transition will occur. The transition would designate NPPD as an operational component within DHS, change its name to Cyber and Infrastructure Protection, and realign the component's programs and functions. The transition is necessary to improve component management and to utilize the component's national operational activities in a way that will meet the evolving requirements of the cybersecurity and critical infrastructure mission. NPPD has invested significant time over the last two years refining the strategic transition objectives and developing the plan to achieve those objectives. The next stage is to work with Congress to authorize and implement the plan.

The transition will improve the component's operational focus and strengthen internal coordination between distinct, but heavily linked, areas of operational activity. NPPD will consolidate current operational activities into three subcomponents: the National Cybersecurity and Communications Integration Center, Infrastructure Security, and the Federal Protective Service. These subcomponents will be supported by centralized mission support functions that provide acquisition, business, strategic, and analytical services. The mission support functions will provide much needed component-wide governance, oversight, and coordination, with more efficient standardized processes and procedures. The need for, and the benefits of, the transition is outlined in Section I. Section II details the current organizational structure, the proposed organizational structure, and the alternatives analyzed as part of our implementation planning efforts.

Section III provides information on the known transition dependencies and challenges. The challenges are largely the result of the continuing evolution of the cyber and infrastructure protection mission over the last decade. The organizational transformation will be challenging but mission requirements, and the expected benefits of this plan, mandate change. Sections IV and V provide detail on risks and measures to mitigate those risks.

Section VI sets forth the plan for implementing and achieving this transition, showing key milestones and the dates of completion.

Cyber and Infrastructure Protection Way Ahead

Contents

I. The Case for Change

NPPD's transition is driven by mission requirements reflecting increasing and evolving risks to cyber and critical infrastructure. A growing cyber threat, including potential for significant physical consequences; a heightened terrorist threat that is increasingly local and often aimed at places like malls, theaters, and stadiums; and more extreme weather events that impact critical infrastructure all place new and growing demands on NPPD to be more efficient and effective.

The evolution of NPPD to Cyber and Infrastructure Protection (CIP) has been designed to address the Nation's most critical challenges and security initiatives while taking into account the progress that has been made. The proposed changes to NPPD respond to employee-driven requirements, which are described below:

The proposed changes directly correspond to recommendations for performance improvements made by NPPD staff who participated in working groups under the Mission Integration Cell in 2014 and 2015. The Situational Awareness and Operations Coordination Working Group and the Customer Engagement Working Group made recommendations to leadership that outlined both the organizational and process changes that employees had recommended during the years that NPPD grew from a small headquarters office to an operating component with a nationwide presence. Many of the participating employees already defined their daily work as operational in nature and urged that the organization itself catch up with that reality. They rightly pointed out, based upon direct customer feedback, that the organization had grown up in stovepipes, with customer engagement and service delivery capabilities built separately in both the physical and cyber focused components of the organization, yet both were consistently reaching out to the same companies or sectors, as well as States and municipalities, resulting in confusion and duplication of effort. They also advocated for separation of response and incident management functions from more steady state engagements to better focus efforts and optimize performance in both incidents and steady state.

NPPD has grown, through accumulation of organizations and missions, from 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. The transition will increase unity of effort through organizational changes and a new name that fosters a clearer recognition of a shared mission—securing and enhancing the resilience of critical infrastructure from cyber and physical threats—to which each entity and individual in CIP contributes.

The transition will improve situational awareness across CIP. Instead of separate watch functions for cyber and physical, we will bring these functions together so that we can detect physical manifestations of cyber events as well as physical events that may impact information and communication technologies, systems, and networks. This Operations Coordination and Watch Center will provide DHS leadership and subcomponents with a holistic view of what is happening and operational responses. An enhanced Strategy, Policy, and Plans function will ensure cohesive approaches to policy development and a dynamic strategic environment. A centralized, but embedded, Management function will ensure that key mission support functions are consistently delivered and subject to appropriate oversight and guidance. An Acquisition

Program Management Office will provide acquisition visibility and oversight to CIP leadership and the Department and enable agile acquisition strategies. Embedding Management and Strategy, Policy, and Plans personnel within the subcomponents also will provide a constant feedback loop for the Under Secretary, which not only empowers decisions by the Under Secretary, but also enables the Under Secretary to foster decision-making at the lowest level possible within the organization using the increased situational awareness available to decision-makers.

How the Transition Strengthens the Cybersecurity Mission

The transition will consolidate all technical cyber operational activity into the NCCIC and elevate its mission leadership to the Assistant Secretary-level, thereby ensuring senior-level attention to the growing program demand. This includes programs providing baseline tools (EINSTEIN and Continuous Diagnostics and Mitigation) for civilian government agencies and enhanced technical services (such as the Enhanced Cybersecurity Services program) for the private sector, as well as Automated Information Sharing (AIS) and incident response and mitigation activities (US-CERT and ICS-CERT). Private sector relationships with the NCCIC will continue, including presence on the watch floor and technical information sharing through Information Sharing and Analysis Centers (ISAC) and the Cybersecurity Information Sharing and Collaboration Program.

Strengthening the private sector, state, local, territorial, and tribal (SLTT) efforts to analyze and manage cyber risks, now undertaken within the Office of Cybersecurity and Communications (CS&C) through Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR) and Office of Emergency Communications (OEC), will be integrated with the risk management activities currently done by the Office of Infrastructure Protection (IP), to create a new entity called Infrastructure Security. SECIR's mission builds capacity across the country to prevent or reduce the impacts of cybersecurity incidents, primarily through assessments and education. These important cybersecurity measures inevitably suffer when senior managers are required to focus on responding to incidents, as they are at present on a daily basis. The NCCIC will focus on incident response while Infrastructure Security's new role will ensure Assistant Secretary attentiveness and the ability to enlist the subcomponent's nationwide resources to strengthen cybersecurity preparedness. Instead of trying to engage infrastructure owners and operators across the country on cybersecurity issues using the roughly 80 headquarters and five field employees currently aligned with SECIR, Infrastructure Security will add a force of nearly 700 headquarters and over 300 field personnel to fully assist the cybersecurity mission.

How the Transition Increases the Security and Resilience of the Nation's Critical Infrastructure

The transition will help meet an increasingly localized terrorist threat. Significant improvements in the Nation's ability to keep known and suspected terrorists out of the country has led terrorist groups to focus on inspiring those already in the United States to act. Similarly, improvements in the ability of law enforcement to detect operational activity has reduced the opportunity for large scale attacks on national iconic infrastructure and led to calls by terrorist organizations for homegrown extremists to attack wherever and however they are able. It is increasingly important to ensure that infrastructure owners and operators, including commercial facilities like

sports arenas, shopping malls, movie theaters, and other places the public gathers in cities and towns across the country are aware of the threat and have the capacity to respond appropriately. This 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 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 CIP's headquarters.

In addition, integrating both cyber and physical elements in Infrastructure Security's risk management collaboration with critical infrastructure will provide a more comprehensive approach that reflects the interplay of cyber and physical in the real world. Our organization should reflect the way the private sector is increasingly organized, specifically with a focus on enterprise risk management across all threats and hazards. This is difficult to do if NPPD is "stove-piped" in a manner that separates physical and cyber and outreach to risk managers is fragmented.

The transition also includes strengthening emergency communications by realigning it with Infrastructure Security. Like SECIR, OEC is hampered by CS&C's focus on incident response. The emergency communications mission will benefit by being realigned into Infrastructure Security because of a shared focus on engagement at the local and regional level.

How the Transition Strengthens Protection of Federal Facilities, Employees, and Visitors

Government facilities are one of the 16 critical infrastructure sectors identified in Presidential Policy Directive 21. Expertise, insights, relationships, and data must be shared between the Federal Protective Service (FPS) and the rest of CIP's activities in order to continue to protect the facilities in this sector.

FPS' mission will be strengthened by a greater unity of effort across operational activity in CIP as well. Within government facilities, physical security is interdependent with cybersecurity, so leveraging cyber expertise is essential. Similarly, Infrastructure Security's relationships and expertise across the private sector also can be brought to bear to more effectively coordinate security at Federal facilities and nearby private facilities, as well as in commercially leased properties that house Federal tenant agencies, to better secure both types of facilities. The Operations Coordination and Watch Center and regionalization will help bring this operational coordination and shared situational awareness to the FPS mission.

How the Transition Strengthens Mission Support for Operational Activity

Subcomponents within NPPD currently have their own management and administrative staffs. This results in resource inefficiency and process inconsistency. As a mature operational component, CIP will ensure efficiency and consistency by centralizing professional support staff under single managers. Human capital and acquisitions are examples of where mission support can be strengthened while benefits accrue to the operational entities. Meeting customer requirements will be assured by embedding staff within the operational entities.

II. Organization

A. Current Structure

NPPD was established under Section 872 of the Homeland Security Act to strengthen national risk management efforts for critical infrastructure.[1] NPPD was originally comprised of CS&C, IP, the Office of Risk Management and Analysis, the Office of Intergovernmental Programs, and the United States Visitor and Immigrant Status Indicator Technology (US-VISIT).

Over the years, various offices within NPPD have been modified (e.g., US-VISIT changed to Office of Biometric Identity Management) or realigned to other DHS components (e.g. Risk Management and Analysis and Intergovernmental Programs). NPPD's operational mission significantly grew with the addition of FPS in 2009. Then in 2014, NPPD established the Office of Cyber and Infrastructure Analysis (OCIA). NPPD began as a small headquarters component of a few hundred employees. It is now an operational entity with a federal workforce of more than 3,000 employees, and more than 13,000 contracted Protective Security Officers, stationed across the country and in the territories.

Based on an internal functional review in partnership with DHS headquarters and decisions made by the DHS Deputy's Management Action Group, several programs and activities were proposed to transfer out of NPPD. These transfers were proposed in order to ensure that the new operational component will be focused on enhancing operations directly related to the mission of CIP[2]. These transfers are proposed in the Fiscal Year (FY) 2017 budget request.

NPPD's programs receive strategic direction and mission support from the Office of the Under Secretary and subcomponent mission support functions. Figure 1 depicts the current organizational structure of NPPD and Appendix A outlines the role of each Subcomponent.

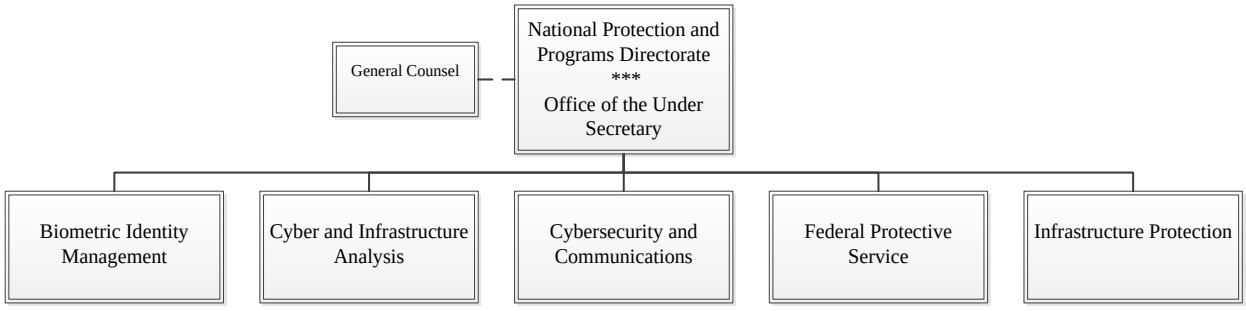

Figure 1 NPPD Organizational Structure

[1] A provision contained in annual appropriations legislation prohibits the Department from using appropriated funds for reorganizing the Department pursuant to section 872 of the Homeland Security Act.

[2] The functions identified in the review which are being proposed to transfer out of NPPD include: the Office of Biometric Identity Management (OBIM); the Office for Bombing Prevention; activities related to cross-Department coordination of Position, Navigation, and Timing; and activities in support of Countering Violent Extremism.

B. Future

DHS seeks to transition NPPD to an operational component called CIP. In the new structure, operations will be carried out through three coordinated subcomponents, each focused on a key aspect of CIP's mission. Figure 2 provides a high level organizational structure for CIP.

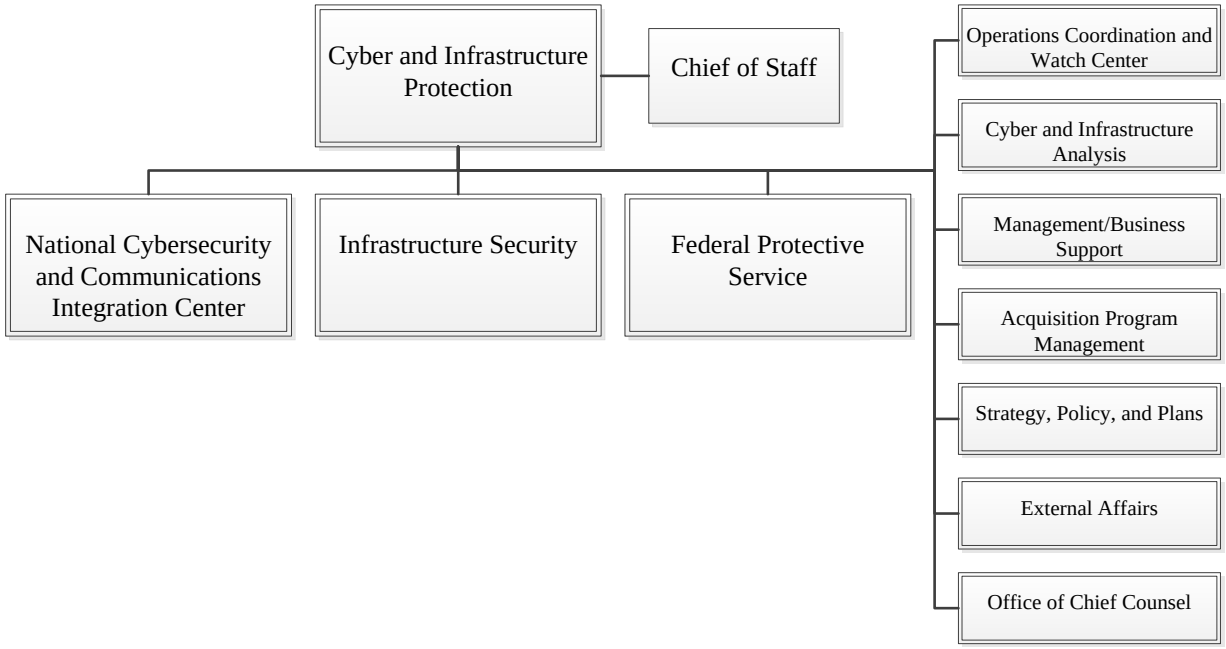

Figure 2 CIP Organizational Structure

Operational Activities

1. THE NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

The first new operational subcomponent will advance the CIP mission through focused operational activity to protect civilian government networks and provide technical cyber information and assistance to SLTT governments, critical infrastructure owners and operators, and the broader cyber ecosystem on which those entities depend. It will be created by elevating the existing NCCIC, to strengthen senior level focus on incidents and mitigation. It will include current programs such as the National Cybersecurity Protection System (NCPS), Continuous Diagnostics and Mitigation (CDM), and innovative program development that address the operational cybersecurity requirements of the federal government, SLTT governments, and the private sector.

The NCCIC will fulfill assigned information sharing, incident coordination and incident response responsibilities in support of the Department, interagency partners, SLTT governments, and the private sector.

The NCCIC will be the primary interface with the Federal civilian executive branch customers for their agencies' cybersecurity issues and will provide technical operational capability as needed. Technical coordination will continue to be facilitated by the private sector's presence in

the NCCIC and through increased interaction with ISACs, other Information Sharing and Analysis Organizations (ISAO) and participants in the Cybersecurity Information Sharing and Collaboration Program.

The NCCIC will be led by an Assistant Secretary and contain three divisions: Federal Network Resilience (FNR), Operations, and Network Security Deployment (NSD). Figure 3 shows the high level organizational structure of NCCIC.

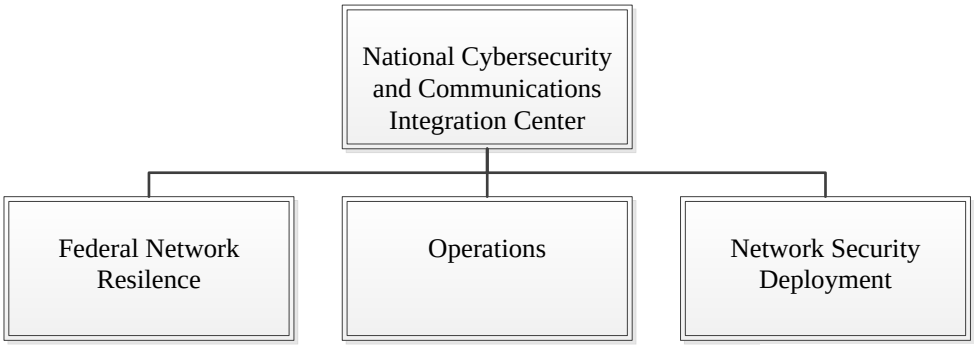

Figure 3 NCCIC Organizational Structure

- **Federal Network Resilience (FNR) -** leads the Department's role in implementing the Federal Information Security Modernization Act (FISMA) and provides civilian federal agencies with guidance and consultative services. FNR manages the annual FISMA reporting and analysis process, which is increasingly leveraging timely and accurate data from sources such as CDM to effectively evaluate each agency's cybersecurity risk. FNR works closely with the Office of Management and Budget to execute a comprehensive governance and oversight regime for federal cybersecurity, including standing evaluations such as CyberStat reviews. FNR also serves as the direct liaison with civilian federal agencies to support implementation of key cybersecurity programs such as CDM and automated indicator sharing. Finally, FNR provides technical guidance and consultative services, including security engineering to help agencies understand how to design their critical systems in a more secure manner.

- **Operations** – serves as the U.S. government's civilian hub for cybersecurity information sharing, incident response, incident coordination, and Emergency Support Function 2-Communications (ESF-2). Operations' customers include all Federal Departments and Agencies, SLTT governments, and the private sector. International entities are key partners to the function of Operations.

  Operations will include several activities that are currently aligned within the existing NCCIC within the current CS&C.

  - United States Computer Emergency Readiness Team (US-CERT) provides on-site or remote assistance to victims of cybersecurity compromises, shares cybersecurity threat, vulnerability and mitigation information, and uses the EINSTEIN system to identify and prevent threats affecting civilian federal

agencies. In the future, it will use data provided by CDM to further enhance its understanding of agencies' risk and support needs.
    - Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) supports the cybersecurity of the nation's control systems, such as those operating power plants and dams. ICS-CERT provides on-site or remote assistance to victims of cybersecurity compromises, promulgates relevant threat and vulnerability information, and conducts training to enhance the ability of control systems professionals to secure and protect their own systems.
    - NCCIC Operations and Integration manages internal tracking and information sharing functions, and it develops and coordinates cybersecurity exercises for federal, private sector, and SLTT customers. Through the National Cybersecurity Assessment and Technical Services (NCATS) team, it conducts vulnerability assessments of federal agencies and private sector partners.
    - The National Coordinating Center for Communications (NCC) is the national lead for Emergency Support Function for communications (ESF-2), and works with telecommunications providers and government partners to support and assure the all-hazards resiliency of the Nation's communications infrastructure.

- **Network Security Deployment (NSD) -** develops, deploys, and sustains cybersecurity technologies to effectively protect federal agencies and the private sector, incorporating innovative approaches that address emerging risks.

    - Among these is NCPS, which includes the intrusion detection and prevention system known as EINSTEIN. NCPS is an integrated system delivering intrusion detection, analytics, intrusion prevention, and information sharing capabilities to civilian federal agencies.
    - NSD also manages the CDM program. CDM provides tools, services, and dashboards to help enable agencies identify and prioritize risks on their own networks.
    - NSD also manages the Enhanced Cybersecurity Services (ECS) program. In ECS, Commercial Security Providers use government-provided classified or otherwise sensitive information to protect their own customers from cybersecurity risks.

2. INFRASTRUCTURE SECURITY

The second new operational subcomponent, Infrastructure Security, will lead CIP's operational efforts to strengthen the ability of owners and operators to manage cyber and physical risks, improve infrastructure resilience, and ensure key national communications capabilities. Infrastructure Security serves as CIP's primary national coordinator for partnerships with the private sector and implementation of the National Infrastructure Protection Plan (NIPP). Infrastructure Security also ensures strong regional and local relationships with owners and operators and state and local governments and other partners that provide partners with comprehensive situational awareness of infrastructure and risk management capacity building services and tools in both steady state and during an incident. These activities include:

- Building and maintaining trusted relationships with owners and operators and delivering risk-informed approaches at a regional level through a robust and integrated field force;
- Leading and expanding engagement with public and private sector groups across the critical infrastructure and public safety communities via activities such as executing Sector Specific Agency responsibilities and facilitating meetings of cross sector advisory groups, including the National Infrastructure Advisory Council, the National Security Telecommunications Advisory Committee, and the National Security and Emergency Preparedness Joint Program Office;
- Applying enterprise risk-management best practices to more effectively mitigate and manage cyber, physical, and human risks to the nation's infrastructure through assessments, promotion of cybersecurity standards and the Critical Infrastructure Cyber Community (C^3) – or "C-cubed" – Voluntary Program, and delivery of training and exercises;
- Ensuring operability of emergency communications and interoperability of first responders' communications capabilities;
- Fostering information sharing among public and private infrastructure owners and operators through programs such as the Protected Critical Infrastructure Information program, Chemical-Terrorism Vulnerability Information program and the Private Sector Clearance Program as well as through strategic threat information sharing efforts and encouraging participation in the NCCIC's technical information sharing programs; and
- Administering the Chemical Facility Anti-Terrorism Standards (CFATS) program to improve the security of the Nation's high-risk chemical facilities.
- Providing standards for physical and cybersecurity of Federal facilities through the work of the Interagency Security Committee.
- Providing on the ground situational awareness and actionable information via steady state activities such as vulnerability assessments, and providing immediate information on infrastructure of concern and potential consequences, lifeline sector infrastructure and protective measures during an incident or period of heightened threat.

Infrastructure Security will be led by an Assistant Secretary, and have six divisions: Emergency Communications; National Security and Resilience Programs; Partnerships; Regional Operations; and Regulatory Compliance; and Technology and Information Protection. These six divisions will work in an integrated manner both within Infrastructure Security and across CIP. Supporting the Infrastructure Security divisions as well as cross-CIP engagement efforts is an Account Executive that serves as coordinator of stakeholder engagement efforts for the entire CIP organization with a focus on ensuring that customers have access to the full range of CIP's capabilities.

As outlined in Figure 4, Infrastructure Security will be structured to allow for improved efficiency among like functions while promoting a collaborative culture across the CIP mission space to foster partnerships, develop and implement programs, and execute emergency communications and regulatory compliance responsibilities.

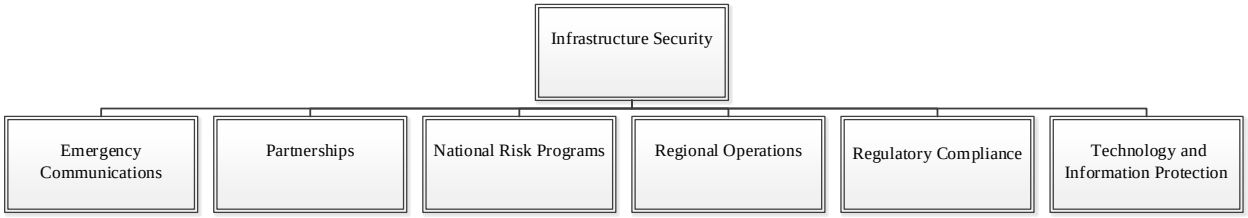

Figure 4 Infrastructure Security Organizational Structure

- **Emergency Communications (OEC) –** executes national policy and programs, as directed by Title 18 of the *Homeland Security Act of 2002* as amended, which are intended to ensure emergency communications and interoperability for first responders and government officials in the event of natural disasters, acts of terrorism, and other man-made disasters. OEC works with the NCC, which leads engagement with communications providers to ensure overall availability of national security and emergency preparedness communication services, on an end-to-end approach to secure communication systems, from land mobile radio to broadband, for emergency responders. OEC, as part of Infrastructure Security, has a specialized technical focus on emergency communications leveraging the priority services programs and standards development and review activities. These priority services are intended to be used in an emergency or crisis situation when the wireless network is congested and the probability of completing a normal call is reduced. OEC leads the development of priority services for voice over Internet Protocol based networks and will continue planning for data and video priority during future budget years.

  The division conducts extensive nationwide outreach to support and promote the ability of emergency responders and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters. It will foster the development of interoperable emergency communications capabilities by SLTT governments and public safety agencies. In addition to this emphasis on engagement with the end users of communications infrastructure, OEC works in close partnership with NCC in its role working with telecommunications services provider.

  Activities from legacy NPPD subcomponents that will align to OEC include: Broadband Deployment on Federal Property Working Group; communications architecture and voluntary consensus standards; continuity of government and communications in coordination with NCC; Emergency Communications Preparedness Center; National Security/Emergency Preparedness Communications Executive Committee; Government Emergency Telecommunications Service program; Interoperable Communications Technical Assistance Program; National Security / Emergency Preparedness Joint Program Office; National Emergency Communications Plan implementation and grant coordination; Next Generation Network Priority Service; priority telecommunications services; promotion of interoperability at all levels of government; promotion of priority telecommunications; SAFECOM; Telecommunications Service Priority; SLTT interoperable communications; Wireless Priority Services.

- **National Security and Resilience Programs –** serves as the program manager for national-level cross-sector cyber and physical risk programs. National Security and Resilience Programs will serve as the central focus for the design, development and measurement of services and products to meet gaps and needs identified through a robust requirements input capability that draws on regional activities, sector engagement and identification of new or emerging risk management priorities. Many of these programs are ultimately delivered by field-based employees through the Infrastructure Security regional structure and/or via the Partnership's Division stakeholder channels. Those programs work to reduce vulnerabilities and mitigate cascading effects when incidents occur, enabling rapid recovery of critical infrastructure.

  Activities from legacy NPPD Subcomponents (IP and CS&C) that align to the National Risk Security and Resilience Programs include education and training to include CIP's active shooter program; assessments methodology and analysis – including the Regional Resilience Assessment Program and physical and cyber assessment tools and data; stakeholder risk assessment and mitigation; exercises; infrastructure development and recovery; cross-sector innovation, capacity building and integration; Interagency Security Committee; Position, Navigation and Timing and Global Positioning Systems risk mitigation; Private Sector Clearance program management; resilience planning; software and supply chain resilience.

- **Partnerships –** promotes, leads, and expands coordinated engagement with public and private sector partners, including public safety partners, who are responsible for the security and resilience of the Nation's critical infrastructure.

  Activities from legacy NPPD subcomponents that align to the Partnerships Division include the following:

  - From CS&C (SECIR) – C^3 Voluntary Program; critical infrastructure stakeholder education and training; cross-sector coordination and integration; Cyber Education and Training Assistance Program; cyber education, cyber training, and higher education; cyber outreach and awareness campaign (Stop. Think. Connect.); Sector Specific Agency management responsibilities, including working with coordinating councils for the Communications and Information Technology Sectors; developing Sector-Specific and Cross-Sector information sharing and collaboration mechanisms; Enduring Security Framework; incident management sector coordination and situational awareness; customer relationship engagement with ISACs and ISAOs in support of CIP information sharing; Network Security Information Exchange management; SLTT strategic cybersecurity engagement; and the National Security / Emergency Preparedness Joint Program Office.
  - From IP – NIPP monitoring (Measurement & Reporting); President's National Infrastructure Advisory Council; President's National Security Telecommunications Advisory Committee; Sector Specific Agency management responsibilities, including working with coordinating councils for the Chemical, Commercial Facilities, Critical Manufacturing, Dams, Emergency Services, and Nuclear Sectors; facilitating Sector-Specific and Cross-Sector information

sharing, and as technical assistance and best practices for the sectors; Sector Specific Plan development and implementation; Sector-specific and cross-sector communications and product development; SLTT Government Engagement; and Threat Information Sharing.
    - From FPS – Sector Specific Agency management responsibilities, including working with coordinating councils for the Government Facilities and the Commercial Facilities Sectors.

- **Regulatory Compliance** – oversees and executes CIP's regulatory programs including high-risk chemical facilities and the sale or transfer of ammonium nitrate. Regulatory Compliance also leads the execution of DHS's responsibilities under *Executive Order 13650: Enhancing Chemical Facility Safety and Security*, leveraging capabilities across the Infrastructure Security organization, to include the partnerships and information sharing forums of the Chemical Sector Councils. It also serves as a co-chair of, and the U.S. lead for, the G7 Global Partnership's Chemical Security Sub-Working Group. Through these activities, the Regulatory Compliance will help ensure that high-risk chemical facilities in the United States are being properly secured. This will make it more difficult for terrorists to acquire improvised explosive device precursors, and will help lead international efforts to establish and maintain a culture of chemical security throughout the world.

  Activities from legacy NPPD subcomponents that will align to Regulatory Compliance include: CFATS oversight, development, and implementation; Ammonium Nitrate Security Program development and implementation; Executive Order 13650: enhancing chemical facility safety and security; G7 Global Partnership Chemical Security Sub Working Group

- **Regional Operations –** operates and executes the Infrastructure Security mission in the field based on established priorities, requirements, and objectives from CIP and Infrastructure Security senior leadership and Infrastructure Security divisions. Regional Operations will include an office at Infrastructure Security headquarters, located within the National Capital Region and 10 Regional Offices across the country, aligned to the Federal Emergency Management Agency (FEMA) regions (Boston, New York, Philadelphia, Atlanta, Chicago, Dallas, Kansas City, Denver, San Francisco/Oakland and Seattle metro areas). The Infrastructure Security Regional Offices (both physical and in organization) will lead, manage, execute and support Infrastructure Security voluntary mission operations and work in an integrated manner with regulatory mission operations. Program goals, strategies, capabilities and performance metrics are established at headquarters, with regional offices working jointly with the headquarters program offices and regional counterparts to ensure goals and operational execution reflect regional requirements.

  Activities from legacy NPPD subcomponents that will align to each regional office include: Protective Security Advisors for the assigned geographic region; Cyber Security Advisors for the assigned geographic region; Chemical Facility Anti-Terrorism Standards chemical security inspectors and field-based activities for the assigned geographic region; emergency communications field-based personnel for the assigned geographic region;

program delivery and customer support functions as identified in the Regional Plan developed under the Office of Infrastructure Protection Regional Planning Team and the CIP Transition Team's planning efforts.

- **Technology and Information Protection –** provides Federal, State, and local governments and private sector stakeholders with innovative information technology (IT) and data protection solutions to efficiently gather, manage, share, and protect physical and cyber risk data for critical infrastructure. These solutions provide a key interface through which DHS mission partners can access a large range of integrated government data, tools, and capabilities to assist in risk reduction, event and incident planning; and enable near-real time situational awareness.

  Activities from legacy NPPD subcomponents that will align to the Technology and Information include: developing and maintaining the IT tools that underpin the physical security and resilience assessment tools; technical operations, maintenance and development of the Communications Assets Survey and Mapping Tool; cybersecurity assessment tools to include the Cyber Infrastructure Survey Tool, External Dependency Management assessments, and the Stakeholder Risk Assessment & Mitigation portal on the IP Gateway; Homeland Security Information Network for Critical Infrastructure (HSIN-CI); Information Technology Investment Governance and Oversight; IP Gateway development, operations and maintenance, and management; Protected Critical Infrastructure Information program management and administration; Chemical Security Assessment Tool (CSAT) suite including the CSAT survey tool and the Chemical Security Evaluation and Compliance System workflow management tool; and Chemical-Terrorism Vulnerability Information Program.

- **Account Executive –** provides integrated situational awareness over stakeholder engagement activities throughout the enterprise. The Account Executive function aggregates customer engagement knowledge and history to better prepare and inform stakeholder activities and strategic engagements across the organization. This includes the identification of new insights and opportunities to enhance the development and delivery of services and products, based on analysis of stakeholder feedback, emerging trends, and other data gathered through external engagements.

  Programs across CIP have distinct missions and purposes, and they are executed at different levels (local, regional, and national). While the different program offices maintain autonomy and flexibility to carry out their individual missions and establish their own relationships, the Account Executive provides a coordinated approach for the entire organization to maintain consistent visibility and awareness of engagement activities across the different mission areas. This is critical for the organization to understand stakeholder engagement activities, leverage relationship management practices, and—whenever practical—consolidate resources and staffing associated with coordination, management, and prioritization of customer engagement efforts. It is also critical to streamline private sector and SLTT interaction with CIP and ensure that the organization is not unduly burdening its partners.

3. FEDERAL PROTECTIVE SERVICE

FPS, the third operational subcomponent, will remain focused on the direct protection of Federal facilities across the Nation and territories but will receive enhanced support from CIP. Through integrated law enforcement and security operations, FPS will continue protecting Federal facilities from the increasing threat. The tenants, visitors, and citizens that depend on the regular function of U.S. Government operations depend on FPS to carry out this critical protection mission every day.

FPS will increase its focus on protecting cybersecurity aspects of Federal facilities in coordination with the NCCIC. In addition, CIP will better integrate all field operations to enable comprehensive security and resilience for CIP stakeholders. FPS will also co-locate incident management support with the Operations Coordination and Watch Center to gain efficiencies and improve situational awareness. FPS will continue serving as a critical element of the Department's counterterrorism mission in protecting infrastructure and those who depend on its security.

Under the new organization, FPS will have three main functions: Operations; Training and Professional Development; and Operations Integration as depicted in Figure 5.

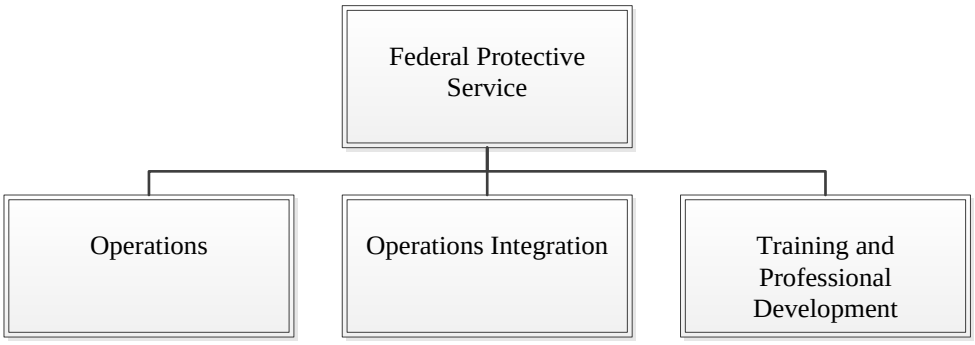

Figure 5 FPS Organizational Structure

- **Operations** – executes the critical protection mission for the organization. It is organized to ensure that FPS can mitigate emerging threats and reduce the overall risk to Federal facilities and the people who rely on them each day. In addition to managing each of the FPS programs, all field execution is managed through this unit.

- **Operations Integration** – ensures that the law enforcement and protection programs integrate and includes activities such as documenting operational requirements and coordinating and deploying new field processes, training, and systems. This unit will also undertake all cross cutting operational issues by engaging with the other CIP operational activities such as: NCCIC on the cyber-physical nexus within Federal facilities; Infrastructure Security on management of the Government Facilities Sector; and OCIA on analytical products. Operations Integration also ensures that the FPS programs have appropriate quality controls and mission compliance through operational readiness and tenant and partnership management activities. Finally, the unit will manage the operational communication and analysis needed to provide service to FPS

tenants and provide for officer safety.

- **Training and Professional Development –** ensures that personnel across the organization have the skills and capabilities necessary to successfully carry out the mission.

Mission Support Activities

To ensure CIP is successful in enhancing operational activity, the organization must execute effective mission support functions. CIP will re-orient its operational and mission support elements by realigning responsibilities and resources to improve support to operations.

4. Operations Coordination and Watch Center

The Operations Coordination and Watch Center (OCW) will be responsible for coordinated operations, joint operational planning, and integrated situational awareness. OCW will build upon the legacy watch and Level 1 Analysis[3] functions of the National Infrastructure Coordinating Center (NICC) Watch, the NCCIC Watch, the FPS Incident Management Cell, and the OCIA Integrated Analysis Cell to enhance leadership situational awareness of the Nation's cyber and physical critical infrastructure. OCW will provide a single point of service for the management of component-wide intelligence information coordination in support of the Key Intelligence Official, coordinate operational planning, and executive briefing functions. OCW will also provide consolidated reporting during steady state, special events, and incident management postures. OCW serves as the connective tissue between the three operational subcomponents to integrate reporting and planning.

OCW will manage component-level continuity of operations and preparedness activities, and to leverage OCW's 24/7 situational awareness/watch function. OCW will ensure near real-time notification to component personnel regarding any emergency incident or event impacting the CIP workforce.

OCW is composed of five divisions (Figure 6).

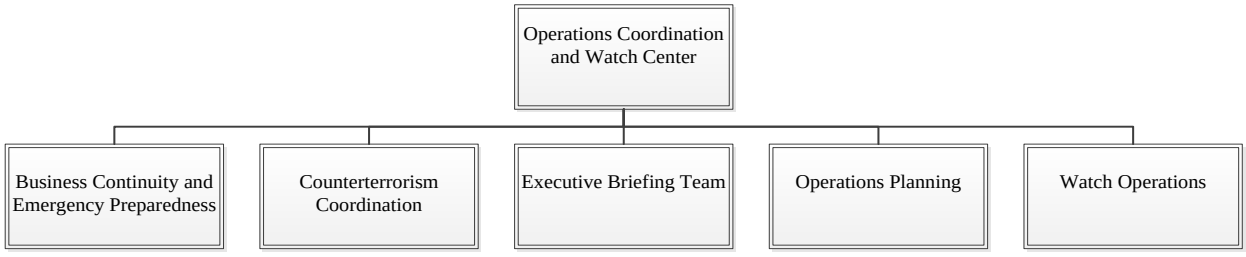

Figure 6 OCW Organizational Structure

[3] "Level 1 Analysis" refers to operational processes and procedures (including monitoring, analyzing, synthesizing multiple information sources, escalating, and tracking and communicating incident details until resolution) executed upon notification or detection of an incident; Level 1 Analysis is conducted up to 24 hours after an incident. "Level 2 Analysis" refers to incident analysis that would require a surge of incident management response staff after the initial 24-hour period; the term "Level 3 Analysis" refers to strategic-level analysis.

- **Business Continuity and Emergency Preparedness –** oversees the component's continuity and employee preparedness programs to ensure continuous execution of the CIP mission.
- **Counterterrorism Coordination –** serves as CIP's lead for coordinating operational counterterrorism (CT) activities in response to emerging threats, and supports CIP leadership's role on the Department's Counterterrorism Advisory Board. In addition, the CT Coordination Cell consolidates operational CT information from across the component and disseminates that information to appropriate stakeholders within CIP and throughout the Department and the Interagency, as appropriate, to ensure CIP's CT activities are transparent, coordinated, and appropriate.
- **Executive Briefing Team (EBT) –** provides senior leadership briefings and talking points (including recommended courses of action) during steady state, incident management, and special events postures. The EBT also provides decision support for actual and impending events and incidents, developed in coordination with subject matter experts from across the component.
- **Operations Planning –** coordinates cross-program/region/subcomponent operational planning, develops and maintains the component Suite of Plans, supports component leadership operational planning priorities, and represents the component in Department and interagency operational planning initiatives.
- **Watch Operations –** monitors, analyzes, and synthesizes information from various sources regarding incidents affecting CIP mission and ensures incident details are tracked and communicated within the Department upon notification or awareness of an incident up to 24 hours after the incident. OCW Watch Operations will consolidate the "like" functions of the legacy NPPD watch organizations (the NICC Watch, NCCIC Watch, FPS Incident Management Center, and OCIA Integrated Analysis Cell) to streamline responsibilities mandated in Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, and Executive Order 13636, *Improving Critical Infrastructure Security*. OCW watch operations will also support regional field operations and provide request for information and requires for additional field force coordination to meet surge requirements.

5. Office of Cyber and Infrastructure Analysis

OCIA will provide consequence analysis, modeling, and prioritization of risks. OCIA will continue to provide essential analysis to support coordinated operational planning and joint situational awareness for CIP and other entities.

OCIA's capabilities are distributed among four primary divisions (Figure 7)— Operational Analysis, Prioritization and Modeling, Production Management and Training, and Strategic Infrastructure Analysis—that work together to provide decision support analysis for internal and external stakeholders, including CIP, DHS, and other Federal, State, local and private sector partners.

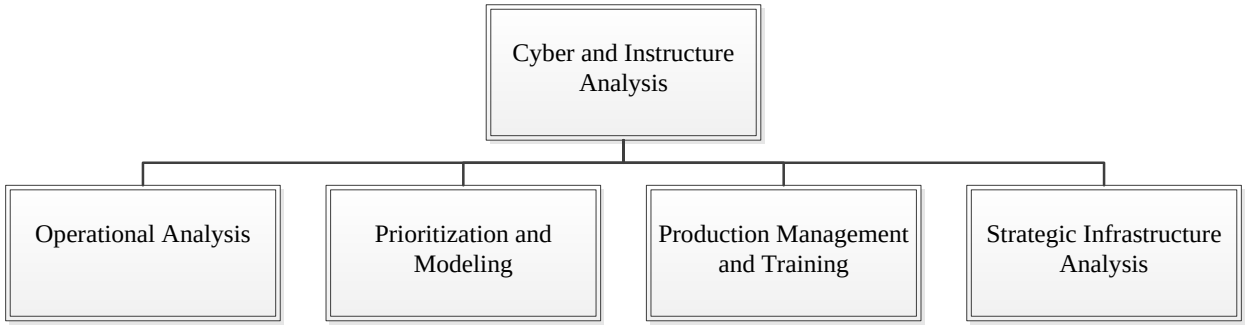

Figure 7 OCIA Organizational Structure

- **Operational Analysis –** supports DHS and CIP Leadership, operational components, and field personnel during crises, emerging threats, or incidents impacting the nation's infrastructure. In its first year of operations, OCIA established the Integrated Analysis Cell, under Operational Analysis, to serve as the intersection between NICC and NCCIC to enhance identification, characterization, and coordination to analyze the cross-sector impact and consequences between cyber incidents affecting infrastructure and physical incidents affecting information and communications technology by an incident or threat. The Integrated Analysis Cell also supports CIP and its stakeholders by producing real-time consequence analysis with over 1,200 cyber-physical analytic responses disseminated to the NCCIC and NICC to-date.
- **Prioritization and Modeling –** provides actionable and timely information to understand the impact and cascading effects of infrastructure failures and disruptions to partners across DHS and its stakeholders as well as other Executive Branch agencies. These partnerships greatly enhance OCIA's integrated consequence analysis of critical infrastructure.
- **Production Management and Training –** collaborates with analysts across OCIA to ensure OCIA products meet analytic tradecraft standards and develops consistent and engaging graphics and visualizations. Production Management and Training also coordinates and delivers analytic trainings to enhance and refine the competency of OCIA analysts and CIP partners.
- **Strategic Infrastructure Analysis –** provides strategic analysis of emerging and future risks to critical infrastructure across sectors and regions, leveraging various national laboratories and working closely with CIP stakeholders and partners.

6. ACQUISITION PROGRAM MANAGEMENT OFFICE

NPPD relies on a number of acquisitions programs to effectively advance its mission. These programs include key programs to provide necessary tools and services to enhance security of Federal networks and systems, provide communications surety, protect Federal and chemical facilities, and enable its analytic and capacity building efforts. However, in NPPD's current structure, many acquisitions functions are dispersed across subcomponents, hampering oversight and consistency. Some key acquisition functions are sometimes "other duties as assigned" for program staff. The transition plan establishes an Acquisition Program Management Office

(APMO), overseen by the Component Acquisition Executive (CAE). The CAE will report directly to the Under Secretary and to the DHS Chief Acquisition Officer.

In order to provide additional acquisitions competencies across the organization and ensure that programs across CIP receive consistent and clear guidance in managing their acquisitions, the APMO will embed teams of acquisition professionals, called Acquisition Core Teams, into NCCIC, Infrastructure Security, and FPS. Each Acquisition Core Team will consist of an Acquisition Account Manager, Cost Estimator, Logistician, and IT Acquisition Specialist.

In addition, NCCIC, Infrastructure Security, and FPS will each designate a senior official as the Portfolio Manager for programs that include significant acquisition activities. Portfolio Managers will ensure that similar acquisitions are managed holistically and consistently across the organization rather than in silos. The Portfolio Manager will report directly to the operational subcomponent head, with the CAE providing acquisition oversight, as well as overall guidance, training, and input on performance plans and evaluation. There will also be a Portfolio Manager for enterprise services supporting all mission support organizations outside the operational subcomponents. The Portfolio Managers will have operational control over the Acquisition Core Team with the CAE maintaining administrative control. Portfolio Managers also will have input into Acquisition Core Team performance plans and evaluations. The Portfolio Managers and Acquisition Core Teams initially will be created using existing resources identified within the operational subcomponents and APMO.

APMO will work with the DHS Office of the Chief Procurement Officer to establish and maintain contract vehicles to make additional acquisition services available to support program execution. These services would be funded and managed by the program(s).

APMO's organization structure is provided in Figure 8.

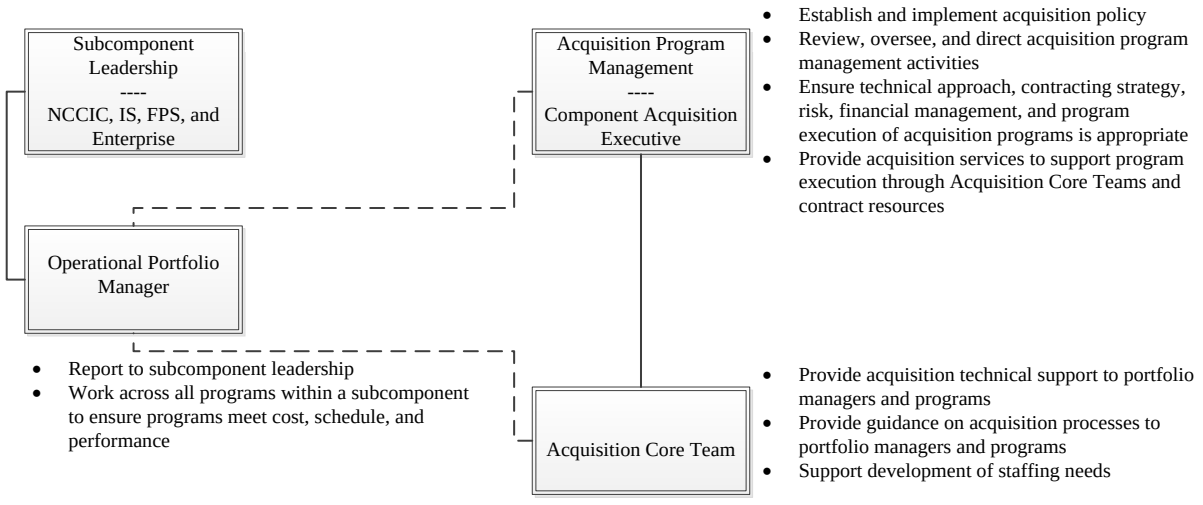

Figure 8 APMO Organizational Structure

7. OTHER MISSION SUPPORT FUNCTIONS

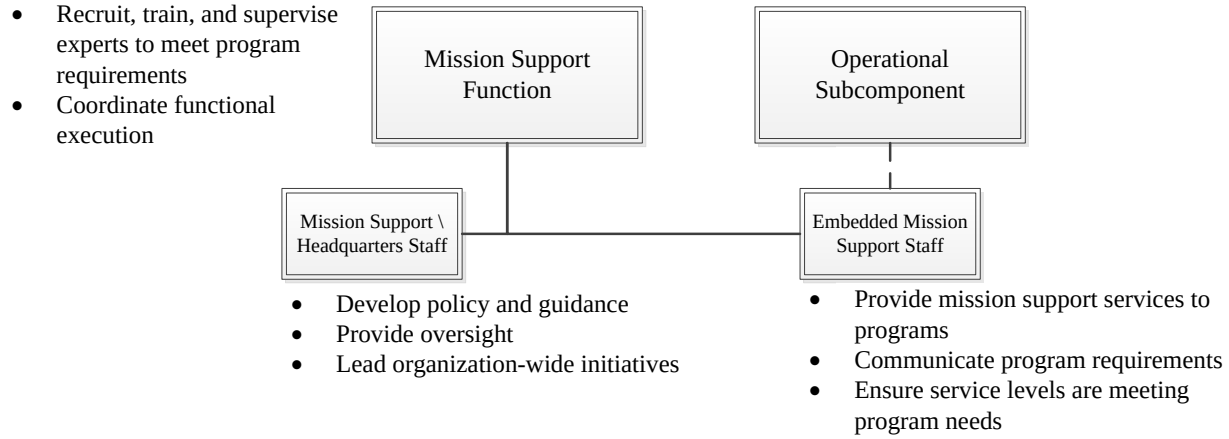

Figure 9 Mission Support Concept

CIP will also strengthen management support by centralizing its other mission support functions, including Management; Strategy, Policy, and Plans; External Affairs; Privacy, Records, and Disclosure; and Chief Counsel. These functions will be accountable to the chief of their respective functions but continue to support their subcomponents in an embedded fashion. In the current NPPD structure, each subcomponent has levels of mission support resources in addition to those in the Office of the Under Secretary. Centralizing the management of these resources will achieve efficiencies through more flexible and dynamic allocation and provide greater accountability for effective support. CIP will ensure the delivery of these services remains focused on supporting operations by establishing Service Level Agreements (SLAs) and embedding staff in the same location as the operators.

Performance of the embedded staff will be managed via SLAs and a governance model that solicits input from the customers. The matrixed business model allows CIP to maintain oversight and ensure consistency in the services provided, while allowing customer requirements to drive the day-to-day activity and customers to provide input on the quality of services being delivered.

Under the matrixed service delivery model, business support services will, in most cases, be embedded and co-located in the headquarters of each operational subcomponent (e.g. FPS, Infrastructure Security, and the NCCIC) as well as division and/or program offices. CIP headquarters will be responsible for delivering comprehensive, coordinated services to the operational entity in an integrated mission support structure. Management will also ensure customer requirements are communicated and achieved throughout its lines of business: Chief Administrative Officer; Chief Financial Officer; Chief Information Officer; Chief Human Capital Officer; and Privacy, Records, and Disclosure. Management staff will work closely with the leads of the operational entities to understand program requirements and communicate these requirements to the line-of-business leads. Additionally, management staff will provide day-to-day operational requirements and direction to the embedded Management team that is able to serve the operational entity's requirements.

Consolidating CIP's mission support functions into a centralized reporting structure with matrixed staff will enhance governance of support functions, increase efficiency, and improve operational support services. More specifically, the objectives are to:

- Provide senior leadership with increased visibility into mission support functions to enable prioritization of initiatives organization-wide and empower executive decision-making;
- Enhance efficiency and unity of effort by providing flexibility to surge resources to support priority initiatives while maintaining operational continuity in mission support service provision organization-wide;
- Centralize governance over like functions to standardize policies, procedures, and execution; and
- Improve customer service by placing the appropriate functions with operational entities to enhance understanding of mission requirements and build relationships between management and operational staff.

Strategy, Policy, and Plans will develop and coordinate CIP strategy and policy, including the management of CIP strategic decision and management processes. Strategy, Policy, and Plans will also integrate CIP strategy and policy activities; provide oversight of operational entity strategy and planning; ensure alignment of plans to CIP-wide directives; design a process for the development of joint requirements; and supply strategy and planning support for subcomponent leadership priorities. Strategy, Policy, and Plans will also manage IG and GAO engagements for all of CIP, track progress against recommendations and ensure close-out of recommendations when appropriate. Finally, Strategy, Policy, and Plans will lead performance improvement initiatives by providing strategic management and operational reviews; developing metrics and reporting on performance; and performing program assessment and process reengineering

External Affairs will provide strategy, planning, coordination, and guidance for cross-cutting communication efforts to enhance communications among entities and organizations across the component, the Department, and the Interagency. It will also oversee the component's public outreach, media, web and digital/social media engagement, and incident communications efforts. Finally, External Affairs will serve as the primary liaison to Members of Congress and their congressional staff.

An Office of Chief Counsel will provide attorneys who focus on component-specific legal needs. The Chief Counsel will obtain appropriate delegated authorities from the General Counsel and will ensure rapid, time-sensitive support on critical matters. NPPD already substantially funds most of its legal support through agreements with DHS Office of General Counsel. During the initial stand-up of the legal office, some service level agreements may be required to continue to address emergent transition-related legal requirements.

The Office of Privacy, Records Management, and Disclosure will be created using staff that currently support privacy, records management, and Freedom of Information Act requests across the organization. This management model mirrors the Department's organizational structure for like functions.

The benefits of this proposal also include enabling NPPD to realize the budget reductions that were included in the FY 2016 budget request and taken by Congress. These efficiencies are detailed in Table 1.

Short Title	FY 2016 Reduction	Explanation
Reductions assuming efficiencies of voluntary partnership activities	$5,010	This reduction assumed that NPPD would consolidate its voluntary infrastructure security and resilience activities and find efficiencies across these activities as they are consolidated.
Reductions assuming enhanced acquisition portfolio management	$3,527	This reduction assumed that NPPD would find efficiencies as it began to look across its assessment tools as a portfolio of investments. This will be critically enabled by the creation of the Acquisition Program Management function.
Reductions assuming mission support efficiencies	$13,096	This reduction assumed that NPPD will realize efficiencies associated with its mission support capabilities as NPPD makes changes to the management structures for its mission support functions.
Total	**$21,633**	

Table 1 FY 2016 Budget Request Efficiencies

Additional challenges associated with the Transition, as well as mitigations, are detailed under Section IV.

C. Analysis of Alternatives

Over the past two years, DHS considered alternatives that would enhance NPPD's internal integration, improve operational effectiveness, and improve acquisitions and management. These efforts included creating the Mission Integration Cell (MIC) at NPPD in June 2014 to study ways to enhance the existing organization and the Process Improvement Team at DHS headquarters evaluating organizational alternatives for how to best ensure NPPD's mission is executed effectively. The two primary alternatives to the proposal in this plan include maintaining the existing organization and focusing on process improvements and other non-organizational changes, as considered by the MIC, or breaking apart NPPD's programs to create a cybersecurity-focused DHS component, which has been proposed by some outside organizations. Ultimately, DHS headquarters decided that the best option was to create CIP, as proposed in this plan. The below summarizes the benefits and costs of the other alternatives examined.

Alternative 1: Status Quo with Process Improvements

NPPD's current structure reflects the disjointed manner in which it was created and evolved, with its subdivisions largely unchanged from their original pre-NPPD structure and operations. The current organization only meets the basic immediate need to provide services that help keep the Nation's critical infrastructure secure and resilient.

NPPD's program oversight, coordination, and business support require improvement. NPPD headquarters currently operates as a holding company for subcomponents that operated largely independently, resulting in missed opportunities and inadequate support for increasingly important mission requirements across the organization. There are duplicative and inefficient layers at multiple levels of the organization due to redundant oversight and business support resources at the subcomponent level, the result of the historic holding-company model.

In 2014 the MIC was asked to make recommendations for improvements within the current organizational structure. After studying options to improve customer engagement, operational coordination, data integration, and business support, the Cell recommended the creation of new coordination functions to integrate operations and improve processes across the organization.

However relying coordination alone would inherently add steps to processes. This would make NPPD less nimble, and ultimately less effective, in supporting incident response activities and working with its customers. In addition, while NPPD has had success in driving process improvements (e.g. decreasing the number of steps in the hiring process from over 50 to fewer than 20), these process improvements take too long to implement and are sometimes undermined due to the redundant oversight and business support layers of the organization.

The current organizational costs are evident in the avoidable inefficiencies and service gaps. For example, in the FY 2016 President's budget request, NPPD proposed $18 million in budget savings assuming that it would defray the costs of its business support functions and outreach activities through consolidation. Further efficiencies cannot be achieved if NPPD continues to

operate in its current structure—the reductions would instead have a programmatic impact and require NPPD to decrease its levels of effort for some mission activities.
The only identifiable benefits of continuing to operate in the current structure would be that it is the path of least resistance. Planning and transition execution efforts would be minimized, and NPPD would be limited to developing practicable support process improvements.

Alternative 2: Create Cybersecurity-Focused Component

DHS also considered the creation of a new cybersecurity-focused component. Under this alternative, the new DHS component would be responsible for the cybersecurity programs that were previously led by NPPD. NPPD would either continue to exist without the Office of Cybersecurity and Communications or NPPD's remaining programs would be divided between other DHS components. This alternative would have the benefit of clearly differentiating the Department's commitment to the cybersecurity mission by creating an organization that solely focuses on this mission, without having to focus on physical threats or biometrics.

DHS concluded that trying to secure infrastructure against cyber risks without considering physical risks and mitigations poses significant vulnerabilities with substantial potential costs. The alternative does not match the way that industry is trending in terms of treating cyber security risk as part of overall enterprise risk management. Moreover, separating cyber from the rest of NPPD also risks separating cyber from the important relationships with critical infrastructure owners and operators that the Office of Infrastructure Protection has developed across the country over many years. Mitigating this cost would require either substantial investment in duplicative efforts or even more robust coordination mechanisms than those referenced in the previous alternative.

The benefits and costs of this alternative are dependent upon the corresponding realignment of NPPD's non-cyber programs. If all other programs remain as part of NPPD, there could be additional mission clarity by providing a purely physical security mission focus. However, having one organization integrate cyber and physical risks holistically will help address the growing cyber threat to critical infrastructure by increasing understanding of risk and ways to mitigate it. CIP must organize the way the private sector is organized to address risks on an enterprise basis.

This alternative also would not strengthen emergency communications. OEC is also hampered by CS&C's focus on incident response and would benefit from being in an organization primarily focused on engagement at the local and regional level and managing consequences from all hazards. Simply breaking out CS&C into a new component would not address this problem.

In addition, critical infrastructure owners and operators will not be well served if there is a federal failure to address the convergence of cyber and physical risks. The growing number of companies who assess and mitigate cyber and physical risks across their respective enterprises would have no counterpart in government. Further since 2007, both the National Infrastructure Advisory Council and the National Security Telecommunication Advisory Council have made recommendations to the President that the approach to infrastructure risk management should be from an enterprise perspective. Moreover, NPPD and the new cybersecurity component would require a net increase of program oversight and business support resources. Each DHS

component has a fixed cost in terms of resources it needs to create a minimum capability, which would need to be duplicated to create a new component. To mitigate these costs, NPPD's remaining programs could be incorporated into other DHS components, but this would also mean that the aforementioned mission clarity would no longer be a benefit as NPPD's infrastructure security mission would be folded into an organization that has historically focused on other matters.

III. Dependencies and Challenges

A. Authorities

One dependency of this plan is the need to modify current statutory authorities. The transition will require legislation that will enable the reallocation of functions within the component and establish the new component name. The legislation would need to amend the Homeland Security Act of 2002 and establish CIP within the Department, led by the Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and other related programs of the Department. The legislation should allow the Secretary to appoint two Assistant Secretaries to assist in carrying out the duties of CIP. Other technical and conforming amendments will be needed to eliminate leadership positions that would no longer exist within the Department and allow for a new reporting structure to accomplish unity of effort within CIP.

B. Department Policy

Department policy will also need to be amended as part of this proposal. DHS Directive 252-01, which addresses the organization of the Department of Homeland Security, would need to be updated to designate CIP as an operational component. Various internal delegations, which vest authority in NPPD leadership to execute and administer their programs and responsibilities, would need to be updated as well to reflect the creation of CIP.

C. Challenges

Managing the Change

A key source of failure of any major change effort is insufficient change management efforts[4]. As a part of an overall change management campaign, NPPD recently conducted a survey of its workforce about its proposed Transition. The survey revealed that employees generally have confidence in in the effectiveness of their direct supervisors, have largely read the Transition Plan, and want to be involved in the Transition and work with others from across the organization. That said, there is work to be done to allow the workforce to internalize and understand the change and how it affects them as individuals and to ensure they are given the tools and resources to continue to conduct NPPD's critical mission.

To address these challenges, NPPD has retained a team of change management experts to provide implementation support and organizational improvement services. The change management team will continue to provide a suite of outreach, project management, change management, obstacle mitigation, and training services. Their efforts will include an enhanced

[4] In its effort to review and refine its strategic objectives and design the organization of the future, NPPD employed the Government Accountability Office (GAO) report entitled, "Results-Oriented Cultures: Implementation Steps to Assist Mergers and Organizational Transformations" (GAO-03-669). CIP will need to continue to employ the key principles of that report and continue to manage and mitigate obstacles to help make the change successful.

communications program to overcome the challenges noted above, as well as the development of specialized training for the NPPD workforce.

Because of the unique nature of NPPD's Transition Effort, this change management methodology is a customized model, using inputs from GAO's Implementation Steps to Assist Mergers and Organizational Transformations (GAO-03-669), John Kotter's Eight Step Change model, Prosci's Three-Phase Process, and the Boston Consulting Group's Change Delta. In brief, the overarching change management strategy will be delivered in three phases that entail:

- Phase 1: Prepare for Change (November 2015 – April 2016)
    - Assess initial organizational readiness
    - Define change management methodology and action plan
    - Establish a sense of urgency and communicate the change vision
    - Strengthen the change coalition
    - Establish key success factors

- Phase 2: Manage Change (Date of Approval – 2018)
    - Develop and execute resistance management
    - Develop and deliver employee training
    - Maintain momentum and morale
    - Assess organizational readiness

- Phase 3: Reinforce Change (FY 2017 – 2019 (assuming approval))
    - Generate continual victories and celebrate success
    - Integrate changes into culture
    - Assess organizational acceptance and measure success factors

The change management effort is well into Phase 1, and continues to work on strengthening the change coalition.

Ensuring Integration across Operational Subcomponents

The new organizational structure will greatly improve CIP program alignment by placing programs organizational dependencies closer together and thereby enhancing collaboration. Programs that move to new operational subcomponents will need to be encouraged to continue cross subcomponent collaboration to ensure that the changes do not adversely impact relationships that were previously advantageous to the mission. For example, after OEC aligns with Infrastructure Security, it will still need to work closely with the NCCIC. In these cases, it will be imperative that CIP ensure that governance structures and processes are in place to provide essential coordination and prevent a decrease in operational effectiveness or duplication of functions.

Creating Matrixed Mission Support Functions

Matrixed organizations enable integration of functions and missions across entities in an efficient manner. However, matrixed organizations can also introduce management challenges including conflicting objectives between different dimensions of the matrix and inadequate processes to

support the management structure. The management challenges of matrixed organizations are widely studied and CIP will adopt best practices to mitigate these challenges. These best practices will include defining service level agreements for matrixed functions; establishing governance structures, processes, and doctrine to oversee matrixed functions; and clearly defining roles and responsibilities between mission support elements and the organizations they support.

Leadership Positions

Consistent with the practices of DHS operational components and other agencies, NPPD will explore the creation of a career Deputy Under Secretary position. This will ensure the continuity of operations by ensuring mission managers remain focused on mission essential functions, operations and incident response and management, while focusing on day to day management and mission support.

Cost

The costs of the proposal will include costs associated with any major organizational change. Staff will be required to devote time to ensuring the success of the Transition that could otherwise be devoted to the mission. In addition, organizational uncertainty can push existing staff to leave for more stable organizations. However, these costs are largely true of the other alternatives.

IV. Impacts to Employees and Support Structures

A. Impact to Positions by Occupation and Grade

NPPD does not anticipate any significant changes in terms of the type of staff it hires or grade levels due to this plan. Roughly 650 CIP employees (excluding functions that are being aligned to different parts of the Department) will be realigned to operational subcomponents or mission support organizations that may have a differing mission from their current organization. About 80 percent of Federal positions within NPPD will not be significantly impacted by the organizational realignment. In most cases, realigned staff members will continue to perform similar job functions as they have in the past, but with improved coordination and engagement across CIP.

FPS union employees will not be realigned. Infrastructure Security Compliance Division union employees will be realigned into Infrastructure Security. Tables 2 and 3 show the alignment of staff in NPPD and in the new CIP organization in FY 2016 and FY 2017.

New Organization (FY 2016 Budgeted FTP)	CS&C	FPS	IP	OCIA	OUS	Total
NCCIC	589					589
Infrastructure Security	187	2	618			807
FPS		1,307				1,307
OCIA				94		94
APM	9	4	1		14	28
Management	94	158	64	16	213	545
SPP	26	5	15	1	16	63
External Affairs	16	4	8	2	10	40
Front Office		1			21	22
OCW	1		35		9	45
Grand Total	**922**	**1,481**	**741**	**113**	**283**	**3,540**
*Does not include Chief Counsel billets currently counted under DHS OGC						

Table 2 Number of staff within NPPD (existing structure) and realignment in total to CIP (new structure) in FY 2016

New Organization (FY 2017 Budgeted FTP)	CS&C	FPS	IP	OCIA	OUS	Total
NCCIC	753					753
Infrastructure Security	201	2	661			864
FPS		1,430				1,430
OCIA				102		102
APM	9	4	1		14	28
Management	94	158	64	16	212	545
SPP	26	5	15	1	16	63

External Affairs	16	4	8	2	10	40
Front Office		1			21	22
OCW	1		35		9	45
Grand Total	**1,100**	**1,604**	**784**	**121**	**282**	**3,892**
*Does not include Chief Counsel billets currently counted under DHS OGC						

Table 3 Number of staff within NPPD (existing structure) and realignment in total to CIP (new structure) in FY 2017

B. Impact to Senior Executive Service Positions

NPPD currently has a cadre of 48 Senior Executive Service (SES) positions, excluding OBIM. This includes 44 career SES positions and three limited-term SES positions, and one Senior Level position. NPPD also requested five additional career SES positions as part of the FY 2016-2017 Biennial Allocations Request to the Office of Personnel Management. NPPD is supported by two career SES positions from the Office of General Counsel that this plan assumes will be transferred into CIP.

These positions, and how they would be aligned in the new organization, are detailed below.

New Organization (FY 2016-2017 FTP)	CS&C	FPS	IP	OCIA	OGC	OUS	Grand Total
NCCIC	11						11
Infrastructure Security	3		7				10
FPS		8					8
OCIA				1			1
APM						1	1
Management			1			5	6
SPP						1	1
External Affairs						1	1
Front Office						7	7
OCW	1						1
Chief Counsel					2		2
Grand Total	**15**	**8**	**8**	**1**	**2**	**15**	**49**

Table 4 Number of SES within NPPD (existing structure) and realignment in total to CIP (new structure)

C. Budget Implications

New Organization (FY 2016 Total $k)	Infrastructure Analysis	Infrastructure Capacity Building	Protect Infrastructure	Management & Administration	O&S Total	Protect Infrastructure	PC&I Total	Infrastructure Capacity Building	Protect Infrastructure	R&D Total	Protect Infrastructure	FPS Total	Grand Total
National Cybersecurity and Communications Integration Center	141,158	45,915	370,580	13,473	571,126	189,173	189,173	2,030		2,030			**762,329**
Infrastructure Security	29,581	173,901	129,972	8,687	342,141	78,550	78,550	3,289	800	4,089	380	380	**425,160**
Federal Protective Service											1,407,539	1,407,539	**1,407,539**
Cyber & Infrastructure Analysis	39,223				39,223								**39,223**
Operations and Watch Coordination	12,082	190	190	2,165	14,627								**14,627**
Acquisitions Program Management	190		1,520	2,541	4,251						760	760	**5,011**
Business Support	7,980	12,540	9,880	56,136	86,536						34,580	34,580	**121,116**
Front Office				3,570	3,570						190	190	**3,760**
Grand Total	**230,214**	**232,546**	**512,142**	**86,572**	**1,061,474**	**267,723**	**267,723**	**5,319**	**800**	**6,119**	**1,443,449**	**1,443,449**	**2,778,765**

Table 5 FY 2016 Budget Request by New Organization, Appropriation, and PPA

New Organization (FY 2017 Total $k)	Infrastructure Analysis	Infrastructure Capacity Building	Protect Infrastructure	Management & Administration	O&S Total	Protect Infrastructure	PC&I Total	Infrastructure Capacity Building	Protect Infrastructure	R&D Total	Protect Infrastructure	FPS Total	Grand Total
National Cybersecurity and Communications Integration Center	198,072	55,490	393,718	13,470	660,750	348,742	348,742	2,030		2,030			**1,011,522**
Infrastructure	26,339	173,668	131,555	7,660	339,222	88,055	88,055	1,639	800	2,439	380	380	**430,096**

Security													
Federal Protective Service											1,415,168	1,415,168	**1,415,168**
Cyber & Infrastructure Analysis	36,404				36,404								**36,404**
Operations and Watch Coordination	14,724	190	190	2,068	17,172								**17,172**
Acquisitions Program Management	190		1,520	2,068	4,127						760	760	**4,887**
Business Support	7,980	12,540	9,880	61,046	91,446						34,580	34,580	**126,026**
Front Office				3,381	3,381						190	190	**3,571**
Grand Total	**283,709**	**241,888**	**536,863**	**90,042**	**1,152,502**	**436,797**	**436,797**	**3,669**	**800**	**4,469**	**1,451,078**	**1,451,078**	**3,044,846**

Table 6 FY 2017 Budget Request by New Organization, Appropriation, and PPA

New Organization (FY 2017 $k)	CS&C	FPS	IP	OCIA	OUS	Grand Total
NCCIC	1,011,522					**1,011,522**
Infrastructure Security	232,580		197,136			**429,716**
FPS		1,415,548				**1,415,548**
OCIA				36,404		**36,404**
APM	1,683	760	190		2,254	**4,887**
Management	17,637	30,020	10,535	4,895	36,808	**99,895**
SPP	4,805	950	2,774	190	2,576	**11,295**
External Affairs	2,986	760	1,368	380	1,610	**7,104**
Front Office		190			3,703	**3,893**
OCW	163		15,560		1,449	**17,172**
Chief Counsel	2,280	2,850	1,520	190	570	**7,410**
Grand Total	**1,273,656**	**1,451,078**	**229,083**	**42,059**	**48,970**	**3,044,846**

Table 7 FY 2017 Budget Request by NPPD Organization and CIP Organization

D. Facilities/IT Requirements

CIP would like to evaluate and consider the feasibility of co-locating CIP headquarters and transitioning to a single IT networks that supports all its operational entities over the long term. No formal proposal has been developed yet pending the resolution of issues such as the personnel footprint to be located on the St. Elizabeths campus, and the disposition of other departmental real estate assets once St. Elizabeths is complete. Creating CIP would impact how personnel are currently located amongst the National Capital Region (NCR) locations, but does not require any significant change to the footprint. NPPD had already planned to create 10 regional offices in the 10 Federal FEMA regions that will in some cases require new facilities. Lastly, as the current footprint is leased and scattered across the NCR; this means that senior leadership and staff spend significant amounts of time in transit to meetings every day. Co-locating CIP headquarters would create significant efficiencies and a consolidated prospectus is being prepared as well as participating in the DHS consolidation planning. Presently NPPD and FPS work under two different information technology (IT) networks. NPPD uses DHS LAN A and FPS is connected with the U.S. Immigration and Customs Enforcement's system. Transitioning to a single IT network that supports all operational entities would avoid any issues related to document sharing, calendar sharing, and e-mail contact databases.

V. Key Milestones

A series of prioritized milestones, established by representatives of CIP's future organizational alignment, will move the overall CIP organization towards its full operating capability.

National Cybersecurity and Communications Integration Center Milestone / Sub-task	Due Date
1. Develop information exchange governance processes between NCCIC and Infrastructure Security regions.	April 2016
2. Transition Enhanced Cybersecurity Services and Cyber Information Sharing and Collaboration Program from SECIR to Enhanced NCCIC	Congressional approval +60 days

Infrastructure Security Milestone / Sub-task	Due Date
1. Conclude analysis of regional field pilot and support requirements analysis	April 2016
2. Implement sustained stakeholder communication effort about organizational changes	June 2016
3. Fully transfer cybersecurity and communications capacity building functions and resources to Infrastructure Security	Congressional approval +60 days

Federal Protective Service Milestone / Sub-task	Due Date
1. Develop Protection Center of Excellence business processes and initial training content	July 2016
2. Co-locate Incident Management personnel with Watch functions on the NCCIC watch floor	October 2016

Management Milestone / Sub-task	Due Date
1. Complete studies of enhanced operational structures and proofs of concept for other lines of business	July 2016
2. Establish interim Service Level Agreements for Management functions	September 2016
3. Establish final Service Level Agreements for Management functions	January 2017 – September 2017

Other Mission Support Functions Milestone / Sub-task	Due Date
I. Co-locate NCCIC, NICC, and OCIA personnel allocated with watch functions into the NCCIC watch floor	December 2015
II. Create task force to improve NPPD External Affairs functions	February 2016
III. Identify acquisition Portfolio Managers and Acquisition Core Team personnel	April 2016
IV. Implement an NPPD Joint Requirements Council	July 2016
V. Transfer NICC and Business Continuity and Emergency Preparedness functions and resources to OCW	Congressional approval +60 days
VI. Implement CIP-wide workforce training plan to reflect new organizational structure and build out expertise	Congressional approval +120 days

VI. Conclusion

This report outlines why and how NPPD will transition to CIP, an operational component of DHS. This transition is necessary to better manage and utilize the national operational activities of the component and meet growing and evolving requirements of the mission to secure infrastructure from cyber and physical risks. NPPD has invested significant time over the last two years confirming the strategic transition objectives, developing the plan to achieve those key objectives, and planning how to manage the changes this transition brings about. This transition also incorporates employee feedback collected during this planning phase, and acknowledges that employees understand that the CIP mission is essential for national and economic security and the importance of their work to drive the organization to a more integrated approach, given the evolving threat and risk environment.

This report reflects the following conclusions:

- The transition is necessary to improve component management and to fully utilize the component's national operational activities in a way that will meet the evolving requirements of the cyber and critical infrastructure mission.
- The transition will improve the component's operational focus and strengthen internal coordination between distinct, but heavily linked, areas of operational activity. CIP will consolidate current operational activities into three subcomponents: the National Cybersecurity and Communications Integration Center, Infrastructure Security, and the Federal Protective Service. These subcomponents will be supported by centralized mission support functions that provide acquisition, business, strategic, and analytical services.
- The transition meets the current mission execution challenge that is largely the result of the continuing evolution of the mission to secure infrastructure from cyber and physical risks over the last decade. The organizational transformation will be challenging but mission requirements, and the expected benefits of this plan, mandate change.
- The transition reflects a deliberate effort to plan for implementing and achieving these objectives, articulating key milestones and the dates of completion.
- The next step is to work with Congress to authorize and implement the plan.

Appendix A: NPPD's Subcomponents

NPPD currently has five subcomponents:

Biometric Identity Management – provides enterprise-level biometric identity information to DHS and its mission partners by matching, storing, analyzing, and sharing biometric data. The Office:

- Maintains the Department's biometric watch list, used to intercept/identify individuals attempting to misrepresent their identities or conceal criminal, terrorist, or fraudulent activities.
- Leads DHS biometric identity services for DHS, Federal agencies, and State and local law enforcement to support the enforcement of immigration laws, prevent unlawful entry into the United States, secure our borders, and assist in the administration of citizenship and immigration benefits.
- Identifies tens of thousands of known or suspected terrorist and other biometric Watchlist matches every year, and provides forensic support to law enforcement agencies.
- Plays a key role in the development of policy and standards that integrate biometric services for domestic and international governments while protecting privacy and civil liberties.

Cyber and Infrastructure Analysis – provides consolidated all-hazards consequence analysis. The Office:

- Promotes understanding and awareness of cyber and physical critical infrastructure interdependencies and the impact of physical and cyber threats and incidents to critical infrastructure.
- Identifies and prioritizes infrastructure at risk through the use of analytic toolsets and modeling capabilities.

Cybersecurity and Communications – advances the security, resiliency, and reliability of the nation's cyber and communications infrastructure. The Office:

- Provides a common baseline of security for the civilian Federal Government.
- Increases the adoption of cybersecurity best practices across government and the private sector.
- Serves as the national hub for public-private cybersecurity information sharing.
- Provides incident response to victims of cybersecurity compromises and coordinates the national response to significant cyber incidents.
- Builds a strong cyber ecosystem by shaping the market for innovative security technologies and advancing the cybersecurity workforce.
- Ensures the interoperability and continuity of national security/emergency preparedness communications.

Federal Protective Service – has broad authorities and jurisdiction to prevent, mitigate, investigate, and defeat threats to Federal facilities and the employees who work there. The Service:

- Protects more than 9,000 Federal facilities and 1.4 million Federal employees and visitors throughout the country every day by executing law enforcement authorities provided under 40 USC § 1315.
- Conducts Threat and Facility Security Assessments and provides tenant agencies with recommendations for countermeasures.
- Investigates criminal activity and threats against government employees, safeguards the right to peaceful demonstration, and prevents the introduction of prohibited items into Federal facilities.
- Designs, maintains, and oversees human and technical countermeasures to enhance protection through 13,000 front line contract Protective Security Officers and a dispersed technical countermeasure program.
- Responds to and manages planned and unexpected critical incidents and special events, serving as a key counterterrorism tool through rapid deployment of protection forces.
- Provides active shooter response, training and crime prevention and awareness education and training to facility tenants and stakeholders.

Infrastructure Protection – coordinates the overall national effort to strengthen critical infrastructure security and resilience. The Office:

- Promotes critical infrastructure risk management at the sector, regional, and individual owner/operator levels, through assessments and identification of risk mitigation measures, information sharing, and partnership and capacity building.
- Oversees the regulation of security at high-risk chemical facilities.