Network Security Deployment Obligation and Expenditure Report

First and Second Quarters, Fiscal Year 2015

June 16, 2015

Fiscal Year 2015 Report to Congress

Homeland Security

National Protection and Programs Directorate

Message from the Under Secretary

June 16, 2015

I am pleased to present the following "Network Security Deployment Obligation and Expenditure Report" for the first and second quarters of Fiscal Year (FY) 2015, as prepared by the National Protection and Programs Directorate (NPPD).

This document has been compiled in response to language in House Report 113-481 accompanying the *FY 2015 Department of Homeland Security* (DHS) *Appropriations Act* (P.L. 114-4). This report covers obligations and expenditures through March 31, 2015 and provides details about NPPD's plans to expend funds in support of Network Security Deployment (NSD) for federal departments and agencies (D/As).

Pursuant to congressional requirements, this report is being provided to the following Members of Congress:

The Honorable John R. Carter
Chairman, House Appropriations Subcommittee on Homeland Security

The Honorable Lucille Roybal-Allard
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable John Hoeven
Chairman, Senate Appropriations Subcommittee on Homeland Security

The Honorable Jeanne Shaheen
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

If you have any questions, please do not hesitate to contact the Office of Legislative Affairs at (202) 447-5890 or the Department's Chief Financial Officer, Chip Fulghum, at (202) 447-5751.

Sincerely

Suzanne E. Spaulding
Under Secretary
National Protection and Programs Directorate

Executive Summary

DHS's cybersecurity approach, laid out in the 2014 Quadrennial Homeland Security Review, prioritizes collaboration across the homeland security enterprise to address emerging cyber threats to national public and private-sector critical infrastructure and key resources. Although individual D/As implement and oversee their own cybersecurity programs, DHS leads the Federal Government's efforts to safeguard America's infrastructure from threats that can affect national security, public safety, and economic prosperity.

The following report provides obligations and expenditures for NSD through March 31, 2015, which sets forth the programmatic context, requisite objectives, and accomplishments necessary to protect and fortify federal cyber assets and infrastructure under P.L. 114-4.

In support of DHS's mission, NSD works to drive and sustain a safe, secure, and resilient cyber ecosystem through innovative leadership, expertise, and strong strategic partnerships. NSD relies on risk management and cyber incident preparedness, prevention, and response activities to achieve these goals. This broad mission charges DHS with a pivotal role in providing the Federal Government with analysis, intrusion detection and warning, intrusion prevention, incident response, information sharing and collaboration, and vulnerability reduction.

Network Security Deployment Obligation and Expenditure Report
First and Second Quarters, Fiscal Year 2015

Table of Contents

I. Legislative Language

This report is provided in response to House Report 113-481 accompanying the *Fiscal Year* (FY) *2015 Department of Homeland Security* (DHS) *Appropriations Act* (P.L. 114-4).

House Report 113-481 states, in relevant part:

> The Committee recommends $377,500,000 for Network Security Deployment, $190,000 below the amount requested and $4,752,000 below the amount provided in fiscal year 2014. Network Security Deployment manages the National Cybersecurity Protection System (NCPS), operationally known as EINSTEIN, which is an integrated intrusion detection, analytics, information sharing, and intrusion prevention system utilizing hardware, software, and other components to support DHS cybersecurity responsibilities. …
>
> The Committee includes a general provision directing the CFO, in conjunction with NPPD, to submit a report detailing the obligation and expenditure of funds not later than 45 days after the date of enactment of this Act, and quarterly thereafter.

II. Network Security Deployment Program Overview

A. Purpose

P.L. 114-4 provided NPPD with $377,000,000 for Network Security Deployment (NSD) to continue the planned procurement of the National Cybersecurity Protection System (NCPS), operationally known as EINSTEIN. EINSTEIN is an integrated system of intrusion detection, analytics, intrusion prevention, and information-sharing capabilities used to defend the information technology (IT) infrastructure of federal civilian Departments and agencies (D/As). The context, requisite objectives, and planned activities necessary to protect and fortify federal cyber assets and infrastructure are detailed herein, as required.

B. Background and Strategic Context

NPPD is responsible for enhancing the protection of federal civilian D/A's IT infrastructure from cyber threats. To achieve this mission, NSD develops, deploys, and sustains the NCPS. NCPS is an integrated system delivering intrusion detection, analytics, intrusion prevention, and information-sharing capabilities to public and private stakeholder groups across the homeland security enterprise.

C. Mission and Vision

NSD's mission is to improve cybersecurity for federal D/As and partners. To meet this mission, NSD designs, develops, deploys, and sustains the NCPS, which provides intrusion detection, advanced analytics, information sharing, and intrusion prevention capabilities that combat and mitigate cyber threats to the federal executive branch information and networks.

NSD's vision is to work collaboratively with federal, state, and local governments and private-sector and international partners to protect and secure cyberspace and America's critical information infrastructure.

The NCPS Program meets this mission through capabilities spanning four broad technology areas:

- **Analytics** – The NCPS Analytics capability provides NPPD's Office of Cybersecurity and Communication (CS&C) cybersecurity analysts with the ability to compile and analyze information in multiple security enclaves about cyber activity, and to inform the public about current and potential cybersecurity threats and vulnerabilities. Analytics provides a Security Information and Event

Management (SIEM) solution for NCPS. The SIEM solution simplifies cyber analysis by aggregating similar events, thereby reducing duplication; correlating related events that might otherwise go unnoticed; and providing visualization capabilities, thus making it easier to see relationships. The Analytics capability also includes Packet Capture tools, a malware analysis laboratory, flow visualization tools, incident management and response tools, and high input/output databases that allow for the analysis of large data sets.

- **Information Sharing** – NCPS-Information Sharing capabilities establish a flexible set of capabilities, implemented at multiple classification levels that will allow for the rapid exchange of cyber threat and cyber incident information among DHS cybersecurity analysts and their cybersecurity partners. The objective of the Information Sharing capability is to: (1) prevent cybersecurity incidents from occurring through improved sharing of threat information; (2) reduce the time to respond to incidents through improved coordination and collaboration capabilities; and (3) improve efficiencies through the use of more automated information sharing and through the disclosure of analysis capabilities. Information Sharing provides a secure environment for sharing cybersecurity information with a wide range of security operations and information-sharing centers across federal, state, local, and tribal governments and private and international boundaries. Information Sharing aims to prevent cybersecurity incidents from occurring by improving coordination and collaboration, automated information sharing, and analysis capabilities in a manner that protects privacy and civil liberties. Additional capabilities under Information Sharing will provide CS&C cybersecurity analysts with a common operating picture (COP) of the threat landscape of federal Executive Branch civilian networks as generated from D/A data sets, ultimately allowing for advanced visualization, analysis and workflow capabilities.

- **Intrusion Detection** – The NCPS Intrusion Detection capability is delivered via EINSTEIN 2 (E2), a passive, signature-based sensor grid that monitors network traffic for malicious activity to and from participating Federal Executive D/As. This capability enables the identification of potential malicious activity and traffic entering or exiting federal networks using a signature-based intrusion detection technology. E2 uses signatures derived from numerous sources such as commercial or public computer security information, incidents reported to the National Cybersecurity and Communications Integration Center (NCCIC), information from federal partners, and/or independent in-depth analysis by the NCCIC. This capability provides CS&C cybersecurity analysts with improved understanding of the network environment and with increased ability to address network weaknesses and vulnerabilities.

- **Intrusion Prevention** – NCPS Intrusion Prevention capabilities will be delivered through EINSTEIN 3 Accelerated (E3A), further advancing the protection of federal civilian D/As by providing active network defense capabilities and the ability to prevent and limit malicious activities from penetrating federal networks and systems. The objective of the NCPS Intrusion Prevention capability is to identify and characterize malicious network traffic to enhance cybersecurity analysis, situational awareness, and security response. It will have the ability to automatically detect and respond appropriately to cyber threats and will support enhanced information sharing by the NCCIC with federal D/As.

III. Network Security Deployment Program Capabilities and Expenditure Status

In FY 2015, $377,000,000 was appropriated for NSD. This program, project, and activity (PPA) encompasses the following activities: Intrusion Prevention, Information Sharing, Analytics, Intrusion Detection, Core Infrastructure, and Program Planning and Operations.

The following FY 2015 NSD activities and accomplishments align with the goals developed in the DHS 2014 Quadrennial Homeland Security Review to create a safe, secure, and resilient cyber environment, and to promote cybersecurity knowledge and innovation through innovative leadership, expertise, and strong strategic partnerships.

FY 2015 Enacted	
Capability	**Allocation**
Analytics	47,521,168
Core Infrastructure	33,300,063
Information Sharing	22,712,313
Intrusion Detection	10,651,318
Intrusion Prevention	154,664,319
Program Planning & Operations	88,821,819
Salaries & Benefits	19,329,000
Total Appropriated	**377,000,000**

A. Analytics

Of the FY 2015 budget, $47,521,168 is allocated to support sustainment of NCPS's advanced analytic tool suite, including deploying redundancy capabilities for the Security Incident and Event Management (SIEM) solution.

FY 2015 Planned Accomplishments

- Initiate an advanced analytics proof of concept that uses streaming analytics to discover patterns in live data that includes the processes and tools associated with near real-time analysis of data streams. Analysis conducted on live data from traffic aggregation points will aid in the near real-time or rapid identification of cyber threats, unusual traffic patterns, or deviations from normalized baselines.

- Operate and maintain SIEM, a capability for normalizing and correlating disparate data source events and for providing threat visualization, analytics, and reporting services.

- Operate and maintain the Advanced Malware Analysis Center, which provides an isolated environment for the safe submission of malware samples, supports automated analysis and storage of malware samples, and provides an unattributable network to support malware research.

- Operate and maintain Enhanced Analytics that significantly reduce the amount of effort and time to analyze large data sets and produce cyber analytics reports, and enrich analysis with a wide range of commercial, open source, and organic threat feeds and data sources presented to operators and analysts in a cohesive fashion for quick action.

B. Core Infrastructure

Of the FY 2015 budget, $33,300,063 is allocated to fund the IT systems and facilities enabling delivery of the NCPS's capabilities.

The NCPS Core Infrastructure capability area offers a common operational and development platform to promote interoperability and efficiency across projects. Core Infrastructure consists of the common equipment, systems, software, and services used across NCPS, regardless of the particular project. Core Infrastructure also serves as the foundation upon which project-specific systems and capabilities are built. This includes all classifications levels of the Mission Operating Environment (MOE) that CS&C cybersecurity analysts use to access the information generated from NCPS operational systems, communications infrastructure linking NCPS facilities, the NCPS Development and Test Environment, and the 50,000 square-foot NCPS Operations and Services Center facility that houses a majority of NCPS's operational support.

FY 2015 Planned Accomplishments

- Operate and maintain the Corry Station facility (Pensacola, Florida), which provides an integrated operations, watch, deployment, and sustainment center for CS&C and the NCPS that can operate autonomously as needed, or in a peer-to-peer relationship with Glebe facility cyber operations supporting real-time information sharing.

- Operate and maintain redundant communication lines infrastructure, which increases network survivability by implementing multiple paths to all major NCPS locations.

- Operate and maintain the development and test environment, which provides an environment to perform technology evaluations, support development and integration of new capabilities, and test performance and security compliance.

- Operate and maintain the MOE, which serves as a dedicated network environment allowing the National Cybersecurity and Communications Integration Center (NCCIC)/U.S. Computer Emergency Readiness Team (US-CERT) to protect its core operations in addition to providing cross-agency infrastructure assurance and cybersecurity services.

- Operate and maintain the Top Secret MOE (TS-MOE), which serves as a dedicated classified network environment allowing the National Cybersecurity and Communications Integration Center (NCCIC)/U.S. Computer Emergency Readiness Team (US-CERT) to exchange information with Service Providers in support of E3A and Enhanced Cybersecurity Services (ECS) programs.

C. Information Sharing

Of the FY 2015 budget, $22,712,313 is allocated to support information-sharing efforts aimed at protecting federal and private-sector critical infrastructure.

FY 2015 Planned Accomplishments

- Deploy additional capability spins of the Cyber Indicators Repository (CIR) and Cyber Indicators Analysis Platform (CIAP), which provides a central repository within the cyber community for indicators and warnings data while protecting attribution through strict access controls and rules on how summary information is reported and supporting internal analysis through the flexible association of structured and unstructured data.

- Continue to operate NCCIC's publically accessible website that provides high-level information about cyber threats. Provided a mechanism for sharing cyber threat advisories and cybersecurity best practices with the general public and for submission of cyber incidents and malware by private citizens.

- Continue to operate US-CERT Portal, a secure portal that is used by DHS and its cyber partners to support information sharing

- Implement a new capability supporting NCCIC's operational needs to enable machine- to-machine sharing of cyber threat indicators with the Information Sharing and Analysis Center (ISAC) community, utilizing Structured Threat

Indicator Exchange (STIX) and Trusted Automated Exchange of Indicator Information (TAXII) standards.

- Plan the deployment of a foundational set of infrastructure capabilities for information sharing (referred to as Block 2.2), such as a secure external application and secure data ingest and sharing hosting environment, Identity Credentialing and Access Management infrastructure, portal services, and data management services supporting the pressing operational needs of DHS and its interaction with key constituencies.

- Plan to host the unclassified Enhanced Shared Situational Awareness (ESSA) Storefront, which provides federated querying of participating national cyber center's shared cyber threat indicators. Develop a plan of action and milestones to implement the President's priority for Automated Indicator Sharing (AIS) capabilities.

D. Intrusion Detection

Of the FY 2015 budget, $10,651,318 is allocated to support sustainment of EINSTEIN 1 and 2 technologies and provide for EINSTEIN 2 expansion to D/As signing new memoranda of agreement (MOAs) for detection services.

FY 2015 Planned Accomplishments:

- Monitor the EINSTEIN 2 sensors deployed at 17 Trusted Internet Connections Access Providers and 4 Managed Trusted Internet Protocol Services service providers, providing EINSTEIN 2 coverage to 81 D/As.

- Monitor traffic for 83 percent of .gov with a total daily average of approximately 23,167 alerts during the second quarter of FY 2015.
  - There were a total of 2,061,892 alerts in the second quarter.

- Conduct technical refresh of EINSTEIN 2 equipment on a scheduled life-cycle basis.

E. Intrusion Prevention

Of the FY 2015 budget, $154,664,319 is allocated to support the continued expansion of NCPS's active defense capabilities for all federal network traffic.

Intrusion Prevention includes elements of NSD's EINSTEIN 3 Accelerated (E3A) effort. E3A improves the protection of federal civilian D/As by providing active network

defense capabilities and the ability to prevent and limit malicious activities from penetrating federal networks and systems. With this capability, NPPD will be able to automatically detect and respond to cyber threats. E3A will conduct intrusion prevention and threat-based decision making on network traffic entering or leaving federal civilian networks. Intrusion Prevention includes Internet service provider (ISP)-supplied intrusion prevention security services and traffic aggregation capabilities, as well as an intrusion prevention analytics capability.

FY 2015 Planned Accomplishments:

- Continue efforts to award traffic aggregation (Nest) Indefinite Delivery/Indefinite Quantity (IDIQ) contracts to the Tier 1 ISPs.
  - Continue operations and maintenance for two Nests that were operational at the start of FY2015
  - The third Nest achieved "Nest Ready" in January 2015.
  - Continue to work with the fourth ISP to achieve "Nest Ready" in FY 2015

- Continue to work contracting efforts with four Tier 1 ISPs for deploying intrusion prevention security services (IPSS).
  - Currently, three of the five Tier 1 ISPs are under contract to deliver initial IPSS capabilities (DNS/SMTP) and design towards future capabilities (in line solutions integrating IPSS capabilities into Nest services and introducing new capabilities, e.g., Web Content Filtering). The first IPSS contract was awarded in March 2013; the second awarded in March 2014; the third in November 2014
  - One ISP is operational with both DNS and SMTP protection services provisioned to 13 D/As
  - A second ISP has received their Authority to Operate (ATO) in February 2015 and is expected to provision their services to D/As in 3Q FY 2015.

- Provide DNS or email protection services to 12 D/As, representing approximately 26 percent of the federal executive civilian .gov users.
  - Initial E3A capability was provisioned to the first federal executive civilian D/A in July 2013.

- Received 51 D/A signed NCPS/EINSTEIN MOAs.

F. Program Planning and Operations

Of the FY 2015 budget, $88,821,819 is allocated to fund operations support services common across all NCPS capability areas.

These services include program management, contracts oversight, financial planning, life-cycle cost estimating, strategic and technical planning and assessment functions, and NSD Front Office support services. These activities ensure all NCPS's capabilities are coordinated and delivered effectively and efficiently, and continue evolving to meet ever-changing cyber threats.

FY 2015 Planned Accomplishments

- Update program artifacts for NCPS milestone Acquisition Decision Event (ADE) decisions: the Cost Estimating Baseline Document; Life-cycle Cost Estimate; Operational Requirements Document; Test and Evaluation Management Plan; System Engineering Management Plan; Integrated Logistics Support Plan; Analysis of Alternatives (AoA); and the program's Acquisition Plan.

- Support preparation and evaluation of Engineering Change Requests and Engineering Change Orders initiated by the NCPS user community.

- Assess emerging cyber threats and the plan for NCPS responses to those threats, and developed an AoA for new capabilities.

- Prepare documents for next ADEs: E3A ADE-2C and Block 2.2 ADE-2B.

G. Salary and Benefits

Of the FY 2015 budget, $19,329,000 is allocated for salary and benefits under the NSD PPA, working to hire and retain a skilled civilian Federal Government workforce to accomplish the NCPS mission and values.

Appendices

Appendix A: NSD Funding (FY 2014 Carryover) by Capability

Funding/Budget Capability	FY15 Q1 Actual	FY15 Q2 Actual as of 3/30/15	FY15 Q3 Planned	FY15 Q4 Planned	Total FY15	Obligations YTD as of 3/30/15	Remaining Planned
FY2014/2015 (2-Year)	**37,899,593**	**15,946,476**	**83,485,928**	**-**	**137,331,997**	**53,846,069**	**83,485,928**
Analytics	9,750,000	-	50,603,711	-	60,353,711	9,750,000	50,603,711
Core Infrastructure	1,025,746	7,271,782	2,166,834	-	10,464,362	8,297,528	2,166,834
Information Sharing	1,216,707	2,858,255	13,915,951	-	17,990,913	4,074,962	13,915,951
Intrusion Detection	2,853,739	1,053,410	4,925,000	-	8,832,149	3,907,149	4,925,000
Intrusion Prevention	21,908,964	3,609,060	9,500,360	-	35,018,384	25,518,024	9,500,360
Program Planning & Operations	1,144,437	1,153,969	2,374,071	-	4,672,477	2,298,406	2,374,071
FY2014/2015 (2-Year) Total	**37,899,593**	**15,946,476**	**83,485,928**	**-**	**137,331,997**	**53,846,069**	**83,485,928**

Appendix B: NSD Funding (FY 2015) by Capability

Funding/Budget Capability	FY15 Q1 Actual	FY15 Q2 Actual as of 3/30/15	FY15 Q3 Planned	FY15 Q4 Planned	Total FY15	Obligations YTD as of 3/30/15	Remaining Planned
FY2015 (Annual)	**12,402,563**	**31,685,236**	**63,735,690**	**101,176,512**	**209,000,000**	**44,087,799**	**164,912,201**
Salaries & Benefits	3,657,840	3,683,721	5,993,719	5,993,720	19,329,000	7,341,560	11,987,440
Analytics	-	6,540,678	5,218,866	19,355,861	31,115,405	6,540,678	24,574,727
Core Infrastructure	-	353,505	14,364,764	10,186,300	24,904,569	353,505	24,551,064
Information Sharing	-	7,187,348	3,091,722	-	10,279,070	7,187,348	3,091,722
Intrusion Detection	-	136,752	4,677,434	4,366,038	9,180,225	136,752	9,043,472
Intrusion Prevention	-	3,101,274	5,998,623	25,856,787	34,956,684	3,101,274	31,855,410
Program Planning & Operations	8,744,723	10,681,958	24,390,561	35,417,806	79,235,047	19,426,681	59,808,367
FY2015/2016 (2-Year)	**-**	**-**	**125,054,232**	**42,945,768**	**168,000,000**	**-**	**168,000,000**
Analytics	-	-	16,405,763	-	16,405,763	-	16,405,763
Core Infrastructure	-	-	7,744,494	651,000	8,395,494	-	8,395,494
Information Sharing	-	-	12,086,518	346,725	12,433,243	-	12,433,243
Intrusion Detection	-	-	1,471,093	-	1,471,093	-	1,471,093
Intrusion Prevention	-	-	78,707,635	41,000,000	119,707,635	-	119,707,635
Program Planning & Operations	-	-	8,638,729	948,043	9,586,772	-	9,586,772
FY2015 Total	**12,402,563**	**31,685,236**	**188,789,921**	**144,122,280**	**377,000,000**	**44,087,799**	**332,912,201**