# Network Security Deployment Obligation and Expenditure Report

Fourth Quarter, Fiscal Year 2015

*January 27, 2016*

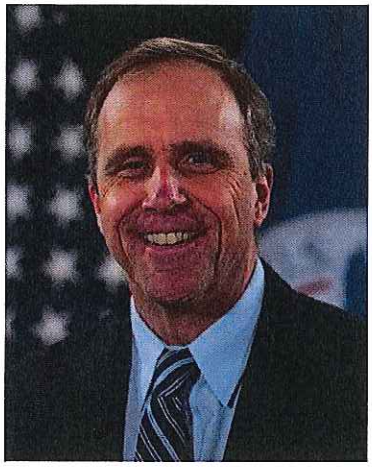
Fiscal Year 2015 Report to Congress

Homeland Security

*National Protection and Programs Directorate*

# Message from the Office of the Chief Financial Officer

January 27, 2016



I am pleased to submit the following "Network Security Deployment Obligation and Expenditure Report" for the fourth quarter of Fiscal Year (FY) 2015, 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) and H.R. 4903. This report covers obligations and expenditures through September 30, 2015, and provides details about NPPD's plans to expend funds in support of Network Security Deployment (NSD) for federal departments and agencies.

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

Inquiries relating to this report may be directed to me at (202) 447-5751.

Sincerely,

Chip Fulghum
Deputy Under Secretary for Management and
Chief Financial Officer

# 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 risks to national public and private-sector critical infrastructure. Although individual departments and agencies implement and oversee their own cybersecurity programs, DHS provides a common baseline of security across the federal civilian government. This baseline of security is provided by the NSD division, within NPPD.

The following report provides obligations and expenditures for NSD through September 30, 2015, including related programmatic context, objectives, and accomplishments as required under P.L. 114-4.

NPPD designs, acquires, and implements cybersecurity solutions to protect the Federal Government and the Nation's critical infrastructure from cybersecurity risks most effectively. In particular, NPPD is charged with implementing the EINSTEIN program to detect and block cybersecurity threats at agency perimeters and the Continuous Diagnostics and Mitigation program to detect and prioritize vulnerabilities inside agency networks. In developing requirements and identifying solutions to manage emerging cybersecurity risks, NSD works closely with the Department's National Cybersecurity and Communications Integration Center, as well as with individual agencies, industry, academia, and other Components within DHS.

# Network Security Deployment Obligation and Expenditure Report
# Fourth Quarter, 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) and H.R. 4903.

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 to the Committees on Appropriations.

# II. Network Security Deployment Obligation and Expenditure Update

Table 1 provides an updated breakout of Network Security Deployment's (NSD) prior-year carryover funding to reflect actual obligations and expenditures through the fourth quarter of FY 2015.

## Table 1: NSD Funding (FY 2014 Carryover) by Capability

| Funding /Budget Capability | FY14 Carryover Planned | FY15 Q1 Actual | FY15 Q2 Actual | FY15 Q3 Actual | FY15 Q4 Actuals | Total FY15 Obligations | Remaining Unobligated Funds |
|---|---|---|---|---|---|---|---|
| **FY2014/2015(2- Year)** | **137,331,977** | **37,899,593** | **15,946,476** | **34,435,407** | **49,047,108** | **137,328,584** | **3,393** |
| Analytics | 55,002,503 | 9,750,000 | - | 29,105,503 | 16,147,000 | 55,002,503 | - |
| Core Infrastructure | 14,759,875 | 1,025,746 | 7,271,782 | 4,562,443 | 1,899,904 | 14,759,875 | - |
| Information Sharing | 17,846,962 | 1,216,707 | 2,858,255 | - | 13,772,000 | 17,846,962 | - |
| Intrusion Detection | 8,832,149 | 2,853,739 | 1,053,410 | 650,000 | 4,275,000 | 8,832,149 | - |
| Intrusion Prevention | 36,096,316 | 21,908,964 | 3,609,060 | 89 | 10,578,203 | 36,096,316 | - |
| Program Planning & Operations | 4,794,172 | 1,144,437 | 1,153,969 | 117,372 | 2,375,001 | 4,790,779 | 3,393 |
| **FY2014/2015 (2- Year) Total** | **137,331,977** | **37,899,593** | **15,946,476** | **34,435,407** | **49,047,108** | **137,328,584** | **3,393** |

Table 2 provides an updated breakout of NSD's FY 2015 appropriated funding to reflect actual obligations and expenditures through the fourth quarter of FY 2015.

## Table 2: NSD Funding (FY 2015) by Capability

| Funding /Budget Capability | FY15 Planned | FY15 Q1 Actual | FY15 Q2 Actual | FY15 Q3 Actual | FY15 Q4 Actual | Total FY15 Obligations* | Remaining Unobligated Funds** |
|---|---|---|---|---|---|---|---|
| **FY2015(Annual)** | **226,912,058** | **12,402,563** | **31,733,170** | **48,788,253** | **133,981,049** | **226,905,035** | **7,023** |
| Salaries and Benefits | 15,085,329 | 3,657,840 | 3,731,655 | 3,718,061 | 3,977,773 | 15,085,329 | - |
| Analytics | 22,805,958 | - | 6,540,678 | 3,612,680 | 12,652,600 | 22,805,958 | - |
| Core Infrastructure | 18,786,897 | - | 353,505 | 11,640,000 | 6,793,392 | 18,786,897 | - |
| Information Sharing | 9,984,905 | - | 7,187,348 | 777,539 | 2,020,018 | 9,984,905 | - |
| Intrusion Detection | 8,477,500 | - | 136,752 | 5,750,000 | 2,590,748 | 8,477,500 | - |
| Intrusion Prevention | 68,567,914 | - | 3,101,274 | 8,770,531 | 56,696,109 | 68,567,914 | - |
| Program Planning & Operations | 83,203,555 | 8,744,723 | 10,681,958 | 14,519,442 | 49,250,409 | 83,196,532 | 7,023 |
| **FY2015/2016 (2-Year)** | **132,087,942** | **-** | **-** | **-** | **89,160,336** | **89,160,336** | **42,927,606** |
| Analytics | 24,587,460 | - | - | - | 19,405,000 | 19,405,000 | 5,182,460 |
| Core Infrastructure | 12,141,879 | - | - | - | 7,712,938 | 7,712,938 | 4,428,941 |
| Information Sharing | 13,048,779 | - | - | - | 9,420,920 | 9,420,920 | 3,627,859 |
| Intrusion Detection | 7,685,738 | - | - | - | 5,815,000 | 5,815,000 | 1,870,738 |
| Intrusion Prevention | 65,104,863 | - | - | - | 40,683,685 | 40,683,685 | 24,421,178 |
| Program Planning & Operations | 9,519,223 | - | - | - | 6,122,793 | 6,122,793 | 3,396,430 |
| **FY2015 Total** | **359,000,000** | **12,402,563** | **31,733,170** | **48,788,253** | **223,141,385** | **316,065,371** | **42,934,629** |

*$18,000,000 of NSD's FY 2015/2016 (2-year funds) was reprogrammed to Continuous Diagnostic Mitigation (CDM) Accelerated Phase 2. The resulting budget available to NCPS was $359,000,000.

** NSD is carrying over $42,927,606 of 2-year funds into FY 2016 and plans to obligate all carryover by FY 2016 Q2.

# III. FY 2015 Accomplishments

## Intrusion Detection

- Monitored the EINSTEIN 2 intrusion detection sensors deployed at 17 Trusted Internet Connections Access Providers and 4 Managed Trusted Internet Protocol Services service providers. EINSTEIN 2 now covers 81 departments and agencies (D/A) and about 93 percent of .gov traffic. These 81 agencies constitute more than 2 million users.
- Conducted technical refresh of EINSTEIN 2 equipment on a scheduled lifecycle basis to ensure that deployed technologies remain best-in-class.

## Information Sharing

- Deployed additional capabilities in the Cyber Indicators Repository and Cyber Indicators Analysis Platform, which provide a central repository for cyber threat indicators and related warnings. These databases are designed to protect attribution through strict access controls and reporting, while supporting robust internal analysis through the flexible association of structured and unstructured data.
- Continued to operate the National Cybersecurity and Communications Integration Center's publicly accessible Web site to share information about cyber threats with government and private-sector partners. The public Web site provides a mechanism to share cyber threat advisories and cybersecurity best practices with the general public and allows the general public to submit reports of cyber incidents and malware for analysis.
- Continued to operate US-CERT Portal, a secure portal used by DHS and its government and private-sector partners for collaborative information sharing about cybersecurity threats and risks.
- Implemented a new capability to enable the near-real-time, machine-to-machine sharing of cyber threat indicators among the private sector and federal D/As for the purposes of network defense, utilizing Structured Threat Indicator Exchange and Trusted Automated Exchange of Indicator Information standards.
- Began to deploy a foundational set of infrastructure capabilities for information sharing (referred to as Block 2.2). This capability will address a pressing operational need of DHS and its partners for secure data ingest, a shared hosting environment, Identity Credentialing and Access Management infrastructure, portal services, and data management services.
- Hosted the unclassified Enhanced Shared Situational Awareness Storefront, which allows DHS and its partners to query databases of cyber threat indicators held by participating government cyber centers.
- Conducted ongoing operation and maintenance of deployed capabilities such as the US-CERT Portal and Cyber Indicators Repository.

## Intrusion Prevention

- Three internet service providers (Century Link (CTL), Verizon (VZ), and AT&T) have operational Nest and Traffic Aggregation services for the EINSTEIN 3 Accelerated (E3A) program. These services provide a platform where DHS can add future protections to the E3A system.
- Two Internet Service Providers (CTL and VZ) are providing operational E3A protections (DNS Sinkholing and Email Filtering).
- Currently, 23 federal civilian D/As are covered by email and DNS protection. These agencies correspond to more than 1 million federal personnel, or 47 percent of the .gov user population.
- Awarded a new contract to CTL that allows any federal civilian agency not currently covered by an E3A provider (CTL, AT&T, and VZ) to gain basic protections. This contract is known as the E3A Service Extension.
- Initiated security assessment of the AT&T E3A infrastructure for the provision of the DNS Sinkholing service in the near-term.
- Continued a pilot with CTL that is examining the effectiveness and scalability of nonsignature-based protections. This pilot is deploying advanced detection capabilities that identified potential cyber threats based upon behavioral characteristics rather than known signatures. Currently, the pilot is covering one agency. On the basis of the results of this pilot, NSD plans to expand to other agencies in FY 2016.
- Worked with CTL to implement infrastructure that will allow the deployment of a third protection: Web Content Filtering.

## Analytics

- Initiated an analytics pilot that will use advanced computation methods to discover potentially malicious traffic in live agency data. This pilot serves as a proof-of-concept to demonstrate the effectiveness of machine learning to detect threats based on patterns and support the discovery of suspicious activity and unknown threats.
- Sustained the Security Information Event Management, Advanced Malware Analysis Center, and Enhanced Analytics capabilities.

## Core Infrastructure

- Sustained core program infrastructure, including the Corry Station facility; redundant infrastructure supporting production, storage, and operational capabilities; the development/test environment; the Mission Operating Environment; and the Top Secret Mission Operating Environment.

## Programming, Planning, and Operations

- Updated program artifacts for the NCPS milestone Acquisition Decision Event (ADE) decisions, including:

    - Cost estimating baseline document; lifecycle cost estimate; operational requirements document; test and evaluation management plan; system engineering management plan; integrated logistics support plan; analysis of alternatives; and the acquisition plan.
    - Prepared documents for next ADEs:  E3A ADE-2C and Block 2.2 ADE-2B.
- Supported preparation and evaluation of engineering change requests and engineering change orders initiated by the NCPS user community.
- Assessed emerging cyber threats, developed a plan on how NCPS will respond to those threats, and developed an analysis of alternatives for new capabilities.

# IV. Budget Execution Changes since Third Quarter Report

## Reprogramming (from the June 30, 2015, reprogramming submission)

The reprogramming of $18,000,000 from NCPS to CDM accelerates the implementation of CDM Phase 2 for all civilian Chief Financial Officer Act D/As. Phase 2 provides software and services that allow DHS and federal agencies to monitor users and their privileges continuously on federal networks. This enables agencies to ensure that users have the appropriate privileges to allow them to complete their work while minimizing user-driven risks, including insider threats.

## Carryover

NCPS carryover at the end of FY 2015 is $42,927,606. This is largely the result of procurement delays due to a contract protest. The funds are planned for obligation by the end of the second quarter of FY 2016.