Department of Homeland Security

Office of Inspector General

Implementation Status of EINSTEIN 3 Accelerated

OIG-14-52

March 2014

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

March 24, 2014

MEMORANDUM FOR: Bobbie Stempfley
Acting Assistant Secretary
Office of Cybersecurity and Communications
National Protection and Programs Directorate

FROM: [redacted]
Acting Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Implementation Status of EINSTEIN 3 Accelerated*

Attached for your information is our final report, *Implementation Status of EINSTEIN 3 Accelerated.* We incorporated the formal comments from the Deputy Under Secretary for Cybersecurity in the final report.

The report contains four recommendations aimed at improving the effectiveness of the EINSTEIN 3 Accelerated program. The National Protection and Programs Directorate concurred with all recommendations. As prescribed by the *Department of Homeland Security Directive 077-01, Follow-Up and Resolutions for Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation.

Based on information provided in management's response to the draft report, we consider all recommendations resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions. Please email a signed PDF copy of all responses and closeout requests to OIGITAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination. Please call me with any questions, or your staff may contact Chiu-Tong Tsang, Director, Information Security Audit Division, at (202) 254-5472.

Attachment

Table of Contents

Appendixes

Abbreviations

E^{3}A	EINSTEIN 3 Accelerated
ISP	Internet service provider
NPPD	National Protection and Programs Directorate
PII	personally identifiable information
US-CERT	United States Computer Emergency Readiness Team

Executive Summary

We audited the National Protection and Programs Directorate's (NPPD) National Cybersecurity Protection System (EINSTEIN 3 Accelerated) that provides an intrusion prevention capability for the Federal Government. Our objectives were to determine its implementation status and whether security and privacy concerns are being addressed to protect the sensitive data processed by the system.

In 2008, NPPD began to deploy the National Cybersecurity Protection System to protect Federal networks and prevent known or suspected cyber threats. NPPD is responsible for the Department's national, non-law enforcement cybersecurity missions. In April 2012, NPPD changed the overall implementation strategy for EINSTEIN 3 Accelerated by procuring commercially-available network defense services. NPPD has begun to deploy EINSTEIN 3 Accelerated to protect Federal networks and expects to reach its full operating capability by the end of fiscal year 2015. In addition, NPPD created its Top Secret Mission Operating Environment, which is a classified network used for EINSTEIN 3 Accelerated analysis. Further, NPPD is finalizing contract negotiations with five Internet service providers to deploy intrusion prevention on 87 percent of Federal agency network traffic. As of September 2013, NPPD established Memorandums of Agreement with 23 Federal agency participants and brought initial protection services to 4 of them. NPPD completed a Privacy Impact Assessment to provide an analysis on how the personally identifiable information collected under EINSTEIN 3 Accelerated will be handled.

Based on our review, we determined that NPPD needs to strengthen the monitoring of the program's implementation and improve the component's ability to handle personally identifiable information as the program matures. Specifically, NPPD must develop implementation measures and a delivery timeline to guide the deployment of intrusion prevention services to its customers on schedule. Further, NPPD must update its training program and standard operating procedure for minimizing personally identifiable information to ensure analysts understand their roles and responsibilities for handling sensitive information. Finally, NPPD must address minor security vulnerabilities identified in its classified operational environment to further reduce risk to sensitive information.

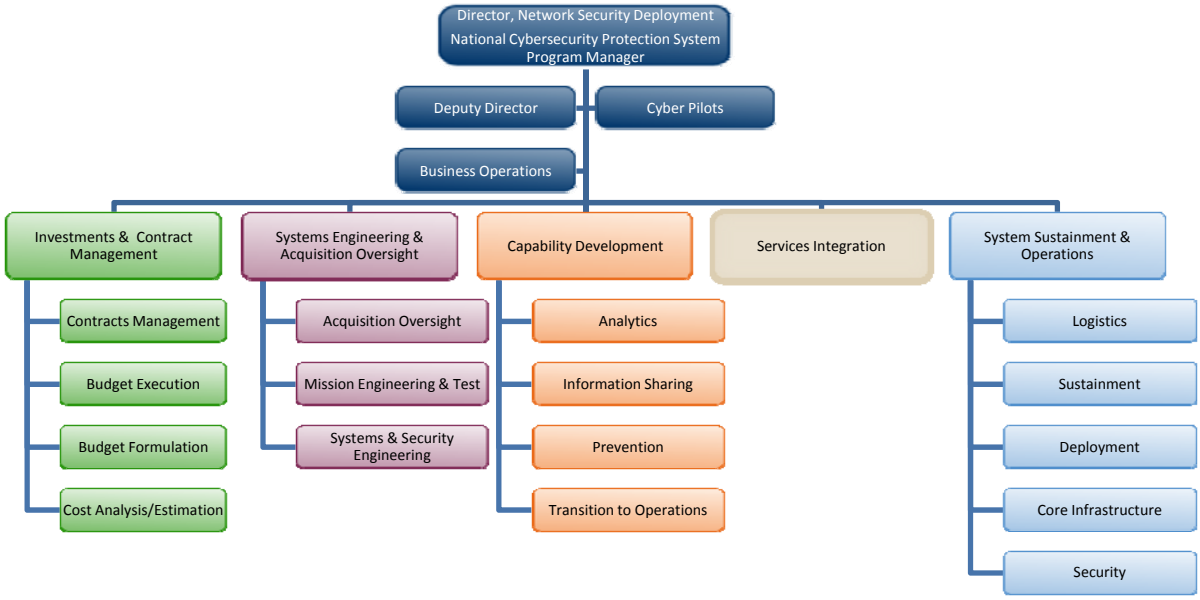
We are making four recommendations to NPPD to help ensure the implementation of EINSTEIN 3 Accelerated proceeds as scheduled and personally identifiable information processed by the system is protected. NPPD concurred with all recommendations and has begun to take actions to implement them. NPPD's responses are summarized and evaluated in the body of this report and included, in their entirety, as appendix B.

Background

The prevalence of cyber attacks—including attempts to gain unauthorized access to information systems or sensitive data stored and processed by these systems—has triggered an expansion of cybersecurity initiatives in the government and private sector. As such, the President has identified cybersecurity as one of the most serious economic and national security challenges we face as a nation. NPPD is primarily responsible for fulfilling the Department of Homeland Security's national, non-law enforcement cybersecurity missions. Through the Office of Cybersecurity and Communications, a sub-component of NPPD, the Department provides crisis management, incident response, and defense against cyber attacks for Federal civil executive branch networks (.gov).

In response to expanding cybersecurity mission requirements from the Administration and Congress, in 2008, NPPD began to deploy the National Cybersecurity Protection System to protect Federal networks and prevent known or suspected cyber threats. Network Security Deployment, which is a division of the Office of Cybersecurity and Communications of NPPD, develops and deploys cybersecurity technologies through the National Cybersecurity Protection System to continuously counter emerging cyber threats and apply effective risk mitigation strategies to detect and deter these threats. Figure 1 depicts the Network Security Deployment organizational chart.

Figure 1. Network Security Deployment Organizational Chart



Source: NPPD

The National Cybersecurity and Communications Integration Center is the operational arm of the Office of Cybersecurity and Communications. Within the National Cybersecurity and Communications Integration Center, the United States Computer Emergency Readiness Team (US-CERT) is responsible for integrating cyber threat information and responding to cyber security incidents that may pose a threat to Federal networks.

In March 2005, NPPD began to deploy sensors (i.e., EINSTEIN 1) on Federal agencies' external Internet connections to collect network flow records passively and fulfill its mandate to act as a central authority for improving the network security of the Federal Government. EINSTEIN 1 is an automated process for collecting network security information from participating Federal agencies. Federal agency participation in the EINSTEIN program became mandatory with the Office of Management and Budget's Trusted Internet Connections initiative in 2007.[1] NPPD began to deploy EINSTEIN 2 in August 2008. EINSTEIN 2 provides intrusion detection capability designed to issue an alert regarding the presence of malicious computer network activity. As of October 2013, EINSTEIN 2 was operational at 17 of 18 Trusted Internet Connection Access Providers and 58 Managed Trusted Internet Protocol Service providers that service Federal agencies participating in the Trusted Internet Connections initiative.[2]

The 2008 Comprehensive National Cybersecurity Initiative requires that the United States expand its EINSTEIN 1 and 2 capabilities to include intrusion prevention functionality across the Federal enterprise. NPPD is in the process of developing and deploying an intrusion prevention capability known as EINSTEIN 3 Accelerated (E^3A) for participating agencies. Prior to E^3A, agencies' intrusion prevention capabilities varied with no standard application of indicators and countermeasures. E^3A combines existing analysis of Federal enterprise-wide EINSTEIN 1 and 2 data and commercial intrusion prevention services to counteract emerging threats. With the adoption of E^3A, NPPD has expanded its role in defending Federal networks with the goal of significantly reducing the avenues of attack available to malicious actors seeking to harm Federal networks.

To defend .gov networks effectively, NPPD requires both passive sensors and proactive protection capabilities that cover the majority of .gov network traffic. E^3A provides the following essential services:

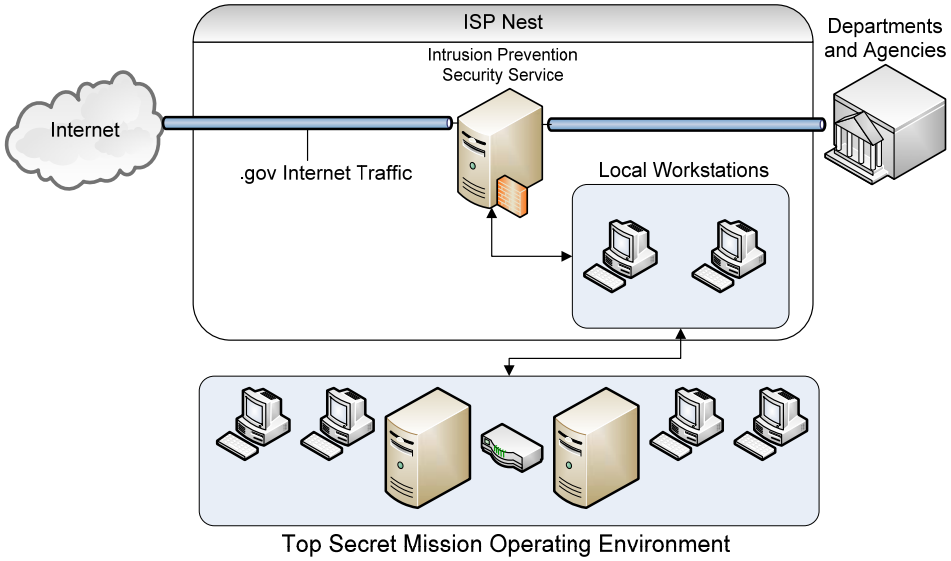
[1] On November 20, 2007 the Office of Management and Budget issued M-08-05, *Implementation of Trusted Internet Connections* which announced the Trusted Internet Connections initiative to optimize individual network services into a common solution for the Federal Government. This solution reduces external Internet connections to improve the security posture of the Federal Government.

[2] EINSTEIN 2 sensors are deployed for Federal agencies participating in the Trusted Internet Connections initiative either as Office of Management and Budget-approved external Internet access points or by contracting with commercial Internet service providers (ISP) through the General Services Administration.

- blocking a detected threat by terminating the network connection or restricting access to the target;
- detecting evasion techniques and duplicating a target's processing;
- removing or replacing malicious code within an attack to make it inoperable;
- disrupting an ongoing attack by implementing security controls and modifying configuration settings in real-time; and
- collecting more detailed information for a specific session after malicious activity has been detected.

The E^{3}A effort encompasses three major components: the Intrusion Prevention Security Service, the Nest, and the Top Secret Mission Operating Environment. The Intrusion Prevention Security Service, which is the core component of E^{3}A, is being procured as a managed service from five ISPs that carry the majority of .gov traffic. ISPs will deploy the Intrusion Prevention Security Service at Nests, which are Top Secret/Sensitive Compartmented Information facilities located at each ISP. Participating Federal agencies enter into a Memorandum of Agreement with NPPD to authorize the deployment of E^{3}A on their networks.[3] Under the direction of NPPD, ISPs administer threat-based decision making on traffic entering and leaving participating Federal networks. The Top Secret Mission Operating Environment is a Top Secret/Sensitive Compartmented Information network that will be used by US-CERT analysts to conduct day-to-day E^{3}A operations, such as receiving, creating, validating, and refining classified and unclassified indicators. Figure 2 depicts the three major components of E^{3}A.

Figure 2. Overview of E^{3}A Capabilities



Source: OIG diagram based on documentation review and interviews with NPPD personnel

[3] The Memorandum of Agreement is approved by the Office of Cybersecurity and Communications.

E^{3}A is built on deep packet inspection of known or suspected cyber threats that are identified from participating Federal agencies' network traffic. Analysts use packet inspection tools to inspect the content of threat data, which may contain personally identifiable information (PII) from or associated with email messages or attachments. To protect PII, NPPD completed a Privacy Impact Assessment on April 19, 2013, to analyze how personal data collected under E^{3}A will be handled. The E^{3}A Privacy Impact Assessment provides details beyond the basic privacy protection measures outlined in the National Cybersecurity Protection System Privacy Impact Assessment dated July 30, 2012. In accordance with standard operating procedures and information handling guidelines, US-CERT analysts are required to review cyber threat information for PII and remove or replace it with a generic label as outlined in standard operating procedures.[4] ISPs administering E^{3}A are required by contract to follow the same PII safeguards.

In June 2007 and August 2010, we evaluated the effectiveness of security controls implemented on EINSTEIN along with other systems supporting the Department of Homeland Security's cybersecurity mission.[5] We reported that NPPD must establish priorities and performance measures to support its mission-critical tasks, ensure all known cyber incidents from across the Federal Government are being reported, and address security issues related to its operational support systems.

Results of Audit

Actions Taken To Deploy E^{3}A

NPPD has made progress towards implementing an intrusion prevention system to protect Federal network traffic. For example, NPPD has taken the following actions:

- Created the Top Secret Mission Operating Environment for E^{3}A analysis capable of processing Top Secret/Sensitive Compartmented Information classified information.
- Established Memorandums of Agreement with 23 Federal agencies as of October 2013.
- Initiated contract negotiations with five ISPs that carry up to 87 percent

[4] If a US-CERT analyst determines that the PII is relevant to the cyber threat, then it will remain as PII. If the indicator associated with the PII is part of a US-CERT product to be disseminated, then the PII is removed.

[5] *Challenges Remain in Securing the Nation's Cyber Infrastructure,* June 2007 (OIG-07-48); *DHS Needs to Improve the Security Posture of Its Cybersecurity Program Systems*, August 2010 (OIG-10-111).

of Federal network traffic. The first contract was awarded on March 29, 2013 and the remaining four are in negotiations. Program officials expect E^{3}A will reach full operating capability by the end of fiscal year 2015.

- Deployed initial intrusion prevention services to the first Federal agency customer on July 24, 2013. NPPD provided these services to three additional Federal agencies as of September 2013. Additionally, the Department of Veterans Affairs provisioned a portion of its network traffic through E^{3}A in October 2013.

NPPD Needs to Address E^{3}A Implementation Issues

We identified issues that NPPD needs to address to strengthen its ability to monitor the execution of the program, and handle PII as the program matures. For example, developing implementation measures can help NPPD deploy E^{3}A within budget and on schedule. In addition, NPPD must provide and document specific, role-based training to educate its analysts on how to properly handle PII under E^{3}A and update its standard operating procedure for minimizing PII to reinforce those skills and help analysts properly understand and exercise their roles and responsibilities. Lastly, NPPD must either address minor vulnerabilities identified on the Top Secret Mission Operating Environment or formally accept the risk and account for them in the system Risk Management Matrix to further protect the PII associated with E^{3}A operations and analysis.

Monitoring of E^{3}A Implementation Needs Improvement

The Network Security Deployment Division needs to strengthen its monitoring of the E^{3}A program's execution by developing implementation measures and a delivery timeline to evaluate ISPs' progress in deploying the intrusion prevention services to protect Federal networks. Federal agencies are required to measure program results through the establishment of program goals and objectives against which progress could be measured. Without developing the implementation measures that can be used to assess progress, increased risk exists that NPPD may not provide intrusion prevention capabilities to customers on schedule.

In April 2012, in response to the National Security Agency's decision to relinquish its responsibilities for delivering a government-off-the-shelf solution for EINSTEIN 3, the Secretary changed the implementation strategy to a managed security service approach (i.e., by procuring commercially available network

defense services). The change in strategy delayed the implementation of the program, caused initial milestones to be missed, and resulted in $86 million in irrecoverable costs. Under the new managed security services approach, NPPD delivered a statement of objectives to five ISPs, along with an Intrusion Prevention Security Service contract and Statement of Work template outlining expected contract language in March 2013. ISPs are required to identify, via Service Delivery Plans, what capabilities they can deliver, and when, to meet intrusion prevention objectives. Based on contract terms, the ISPs are proposing different approaches and milestones to reach full operating capability. NPPD plans to use the Service Delivery Plans to further refine schedule milestones. NPPD officials agreed that their contracting approach carries some risk, but that it best aligns with the goal of quickly deploying E^3A protection services. They indicated that they will be in a better position to manage delivery timelines once contracts are awarded.

NPPD uses an Integrated Master Schedule to monitor the status of high-level tasks for the National Cybersecurity Protection System, including E^3A. The schedule is updated daily and reviewed regularly with project teams and management. In addition, NPPD has developed the following "key performance parameters" to measure the program's maturity at full capability:

- Intrusion prevention signatures shall be developed, tested, and deployed to the ISP in a timely manner.
- E^3A shall protect .gov traffic and provide coverage for subscribers using countermeasures.
- E^3A shall match traffic against signatures accurately.[6]

These performance parameters might be useful in establishing program goals for the procurement of intrusion prevention services, but they are vague as performance measures. Specifically, these parameters need clearly identified milestones or deliverables to measure ISPs' progress in delivering services to Federal agencies. Further, the parameters do not provide enough detail to measure how well the program meets targeted service levels within a particular timeframe.

Federal agencies are required to establish performance goals to define the level of performance to be achieved during the current and subsequent fiscal years. In addition, agencies are to express the goals in an objective, quantifiable, and measurable manner as well as clearly defined milestones. Finally, agencies are

[6] *National Cybersecurity Protection System Acquisition Program Baseline*, Version 3, August 23, 2013.

required to establish a balanced set of performance indicators to be used in measuring or assessing progress toward each performance goal.

E^3A is a complex, multi-million dollar undertaking that encompasses five multi-phase contracts with five different ISPs.[7] The implementation of E^3A includes the development of a support operational network and frequent coordination with more than 23 Federal customers with varying capabilities and needs. In addition, the sophistication and effectiveness of cyber attacks have steadily advanced in recent years. Without developing implementation measures and the delivery timeline to assess progress from five different ISPs, it may be difficult for management to effectively monitor E^3A implementation efforts. Further, there is little assurance that NPPD would be able to deliver intrusion prevention capabilities to participating agencies on schedule.

Recommendation

We recommend that the Acting Assistant Secretary, Office of Cybersecurity and Communications:

Recommendation #1:

Develop implementation measures and a delivery timeline to monitor progress of the E^3A program.

Management Comments and OIG Analysis

NPPD concurred with recommendation 1. The Deputy Under Secretary for Cybersecurity said that the process to define performance measures specific to contract activities prior to contract award will continue for ISPs. NPPD noted that the development and implementation of performance measures was completed with the first ISP at the time of contract award (March 29, 2013). Further, this ISP's schedule for implementing Domain Name Service and Email services was submitted with their proposal and has been tracked weekly by the Program Office. The implementation schedule for the Intrusion Prevention Security Service will be finalized in the fourth quarter of fiscal year 2014.

We agree that the steps NPPD is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open and resolved until

[7] As of August 22, 2013, NPPD has spent more than $321 million to develop and implement its intrusion prevention capability.

NPPD provides supporting documentation that all planned corrective actions are completed.

E^3A PII Handling Requirements Must Be Reinforced through Role-Based Training and Procedures

US-CERT has not received specific, role-based training or updated its standard operating procedure for minimizing PII to ensure the protection of PII in the E^3A program. In particular, the existing training of US-CERT analysts and the current standard operating procedure do not properly specify requirements for handling PII or describe E^3A's evolving operational capabilities. As a result, analysts may not be fully aware of their roles and responsibilities for properly identifying, minimizing, and handling PII, which may lead to information leakage and cause potential embarrassment to the Department.

NPPD developed the National Cybersecurity Protection System Privacy Impact Assessment to outline specific training requirements that must be administered when an analyst comes in contact with information that may contain PII. Further, analysts are required to screen all data and information that they intend to use to determine whether the information contains PII and ensure these personal data are properly handled in accordance with current standard operating procedures and *US-CERT Cybersecurity Information Handling Guidelines*.[8]

However, our review of US-CERT's standard operating procedure for PII handling and minimization revealed that it is insufficient. For example, the procedure has not been finalized and does not contain specific instructions for an analyst to follow to protect and minimize the collection of personal data from E^3A during day-to-day operations.

The NPPD Privacy Office offers a general privacy training course to all NPPD personnel on how to properly handle PII. While the training provides a basic understanding of the need to protect PII, we determined that it does not cover the requirements or day-to-day E^3A operational requirements for analysts to handle PII. According to the NPPD Privacy Office officials, the employees who attend this training satisfy their annual privacy training requirement. In addition, the officials said that, as a supplement to the general privacy training course, analysts are trained on standard operating procedures when they join US-CERT. However, NPPD was unable to provide training content or records of completion.

[8] *US-CERT Cybersecurity Information Handling Guidelines* (August 15, 2013) and *E^3A Privacy Impact Assessment (*April 19, 2013).

A US-CERT official said that the current capabilities of the system and a limited amount of data being processed at this stage of the program do not warrant the need for in-depth analysis and screening for PII. Further, since additional capabilities have yet to be determined, the official said that devoting time and resources to develop unconfirmed training and standard operating procedure topics was unnecessary at this time. The official acknowledged that the training requirements outlined in the National Cybersecurity Protection System Privacy Impact Assessment do not reflect how analysts are currently trained. The official and the E^{3}A Program Manager said that they fully support the development of targeted training topics and standard operating procedure specifications as additional system capabilities are implemented. According to NPPD officials, all US-CERT standard operating procedures are reviewed to ensure consistency with the US-CERT Cybersecurity Information Handling Guidelines.

The *Privacy Act of 1974* requires that agencies not disclose any record which is contained in a system of records by any means of communication to any person, or to another agency except under certain conditions.[9] DHS requires agencies to consider the effects of their actions on the privacy rights of individuals, and ensure that appropriate safeguards are implemented. Any PII that could cause substantial harm, embarrassment, inconvenience, or unfairness to an individual must be protected.

As E^{3}A program capabilities expand, generalized procedures and current training on PII handling may not be sufficient to detect and minimize PII collected by E^{3}A. Additionally, developing and finalizing standard operating procedures focused on the current and subsequent operational capabilities, including E^{3}A, will assist analysts in mitigating and minimizing the possible release of PII by implementing a standardized detection methodology unique to their roles and responsibilities under the program.

Recommendations

We recommend that the Acting Assistant Secretary, Office of Cybersecurity and Communications:

Recommendation #2:

[9] A system of records refers to a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying information assigned to the individual.

Update the PII training program to include the roles and responsibilities for the analysts to identify, minimize, and handle PII under E^3A. A training schedule should be developed and offered periodically.

Recommendation #3:

Revise standard operating procedures to include specifications of current and subsequent E^3A operational capabilities as well as analysts' roles and responsibilities for identifying, minimizing, and handling PII under E^3A.

Management Comments and OIG Analysis

Management Comments to Recommendation #2

NPPD concurred with recommendation 2. The Deputy Under Secretary for Cybersecurity said that the NPPD Office of Privacy is developing role-based training specific to PII handling in coordination with US-CERT to supplement existing PII training. Role-based training will be required annually and conducted quarterly or as often as needed. The National Cybersecurity and Communications Integration Center Oversight and Compliance Officer will schedule and document training. The NPPD Office of Privacy expects to develop role-based training by the third quarter of fiscal year 2014.

OIG Analysis

We agree that the steps NPPD is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open and resolved until NPPD provides supporting documentation that all planned corrective actions are completed.

Management Comments to Recommendation #3

NPPD concurred with recommendation 3. The Deputy Under Secretary for Cybersecurity said that US-CERT reviews and updates its internal standard operating procedures on an ongoing basis. NPPD noted that standard operating procedures are not meant to be "program specific," but, rather, cover activities across US-CERT capabilities and programs. However, as a part of ongoing efforts, US-CERT will specifically identify those programs which are covered in each standard operating procedure.

OIG Analysis

We agree that the steps NPPD is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open and resolved until NPPD provides supporting documentation that all planned corrective actions are

completed.

System Security Controls

Overall, NPPD has implemented effective security controls on its Top Secret Mission Operating Environment. However, NPPD needs to address two minor vulnerabilities and out-of-compliance United States Government Configuration Baseline configuration settings. Further, NPPD has not formally accepted the risk for or documented these vulnerabilities and out-of-compliance configuration settings in the system's Risk Management Matrix.[10] While the identified vulnerabilities and out-of-compliance configuration settings are minimal and do not pose a significant threat to the safety and integrity of the system, unmitigated vulnerabilities may expose the system and the data it processes and stores to potential exploits.

To evaluate the effectiveness of controls implemented on the system, we performed vulnerability assessments on 61 Windows computers to identify missing patches and evaluate United States Government Configuration Baseline compliance and additional security controls.[11] We identified two vulnerabilities that may create opportunities for exploitation of the system. Additionally, we determined that, on average, NPPD has implemented 99.5 percent of the required United States Government Configuration Baseline settings on the system.

We determined that the vulnerabilities identified could be attributed to the improper configuration of software when the system was initially built and incompatibilities among different software products. According to NPPD personnel, the out-of-compliance United States Government Configuration Baseline configuration settings were enabled to allow mission essential functionality during system development. Additionally, NPPD is in the process of formally accepting the risk and accounting for the vulnerabilities in the system's Risk Management Matrix.

Federal agencies are required to implement United States Government Configuration Baseline configuration settings on workstations to standardize and

[10] A Risk Management Matrix captures threats, vulnerabilities, and risks inherent to the operational environment, architecture, or design of an information system.
[11] In March 2007, the Office of Management and Budget issued M-07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*, which requires Federal agencies to adopt the federally accepted configurations developed by National Institute of Standards and Technology, Department of Defense, and the Department of Homeland Security.

strengthen information security across the Federal Government. The *Department of Homeland Security Sensitive Compartmented Information Systems Information Assurance Handbook* provides information on security controls necessary for a system that processes Sensitive Compartmented Information. The Department requires any identified vulnerabilities to be included in the Risk Management Matrix for submission and approval by the Designated Accrediting Authority.

Mitigation of the vulnerabilities we identified will reduce the risk that sensitive information could be compromised. Additionally, failure to accept risk and account for known out-of-compliance configuration settings in the system Risk Management Matrix could deny the Designated Accrediting Authority updated information to make credible, risk-based decisions regarding E^3A.

Recommendation

We recommend that the Acting Assistant Secretary, Office of Cybersecurity and Communications:

Recommendation #4:

Fix the identified vulnerabilities and out-of-compliance configuration settings on the Top Secret Mission Operating Environment or formally accept the residual risks for them in the appropriate Risk Management Matrix.

Management Comments and OIG Analysis

NPPD concurred with recommendation 4. The Deputy Under Secretary for Cybersecurity said that NPPD submitted the required DHS Information Security Program Request for Waivers and Exceptions for all findings to the accrediting authority on November 19, 2013. The exception request submitted states that, while the configuration deviations exist, mitigations are in place to ensure that they pose no direct or indirect threat to the network.

We agree that the steps NPPD is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open and resolved until NPPD provides the approved waiver request to support that the accrediting authority has formally accepted the residual risks of the identified vulnerabilities and out-of-compliance configuration settings.

Appendix A
Objectives, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

The objective of our audit was to determine the implementation status of the National Cybersecurity Protection System (E^3A) and to determine whether security and privacy concerns are addressed to protect the sensitive data collected and processed by the system. Specifically, we determined whether: (1) E^3A is being deployed as scheduled and within budget, (2) effective policies and procedures have been developed to protect the PII collected by and stored on the system, and (3) effective security controls have been implemented to protect the sensitive data collected, processed, and generated by the system.

Our audit focused on requirements specified in the *Federal Information Security Management Act of 2002*, United States Government Configuration Baseline, Office of Management and Budget Circular A-11, *Preparation, Submission and Execution of the Budget*, and Office of Management and Budget Circular A-123, *Management's Responsibilities for Internal Controls,* Office of Management and Budget Circular A-130, *Management of Federal Information Resources*, *Department of Homeland Security Sensitive Systems Handbook 4300A, Department of Homeland Security Sensitive Compartmented Information Systems Information Assurance Handbook, US-CERT Cybersecurity Information Handling Guidelines,* and *US-CERT Standard Operating Procedures 108, 110, 445, 502, 504, 505, and 507*. We interviewed selected personnel from NPPD Privacy Office, National Cybersecurity and Communications Integration Center, and Network Security Deployment to discuss the program implementation schedule, budget and acquisition, policies and procedures, analyst responsibilities, training, and system security controls. We also interviewed selected personnel from an ISP and a Federal agency for their perspective on NPPD's interactions and support functions pertaining to E^3A.

In addition, we reviewed program progress and future plans as well as allocated and requested project funding. We reviewed contracts and Memoranda of Agreement to determine if NPPD has been successful and timely in establishing contracts with ISPs and participating agencies. Further, we reviewed the training, policies, and procedures developed to protect E^3A PII. Finally, we used Tenable Nessus software and manual

technical control checks to identify missing patches and determine compliance with applicable Federal and Department requirements on 61 Windows machines on the Top Secret Mission Operating Environment.

We conducted this performance audit between July 2013 and September 2013 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives. Major Office of Inspector General contributors to the audit are identified in appendix C.

Appendix B
Management Comments to the Draft Report

National Protection and Programs Directorate
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

FEB 25 2014

Mr. Carlton Mann
Chief Operating Officer
Office of Inspector General
U.S. Department of Homeland Security
Washington, DC 20528

Dear Mr. Mann:

Re: Office of Inspector General Report Implementation Status of EINSTEIN 3 Accelerated (OIG Project No. 13-153-ITA-NPPD)

Thank you for the opportunity to review and comment on this draft report.

The Department is pleased to note the Office of Inspector General's (OIG's) acknowledgement that the National Protection and Programs Directorate (NPPD) has made significant progress towards implementing an intrusion prevention system to protect Federal network traffic. For example, NPPD has taken the following actions:

- Created the Top Secret Mission Operating Environment for EINSTEIN 3 Accelerated (E3A) analysis capable of processing Top Secret/Sensitive Compartmented Information (TS/SCI) classified information. NPPD has implemented effective security controls on its Top Secret Mission Operating Environment.
- Established Memorandum of Agreement with 23 Federal agencies as of October 2013.
- Initiated contract negotiations with five Internet Service Providers (ISPs) that carry approximately 87% of Federal network traffic at full capacity. The first contract was awarded on April 1, 2013, and the remaining four are still in negotiations. Full operating capability is expected by the end of fiscal year 2015.
- Deployed initial intrusion prevention services to the first Federal agency customer on July 24, 2013; and to three additional Federal agencies as of September 2013. Additionally, the Department of Veterans Affairs provisioned a portion of its network traffic through E3A in October 2013.
- Conducted and published a Privacy Impact Assessment for the E3A program on April 19, 2013.

The objective of the audit was to determine the implementation status of E3A and whether security and privacy concerns are addressed to protect the sensitive data collected and processed by the system. The fieldwork for the audit was conducted during the early stages of the implementation of the E3A. Fieldwork was initiated on July 10, 2013. At the time of the audit, one ISP was under contract to provide E3A services. The first Department/Agency was provisioned on July 24, 2013. During the fieldwork window, there were two additional

Department/Agency customers provisioned on E3A. All of the agencies provisioned during that time were smaller agencies that would not have produced a considerable amount of activity data. The lack of data available during the assessment window made it difficult for the OIG auditors to assess how E3A data was collected and processed. Since the end of the fieldwork period, the Program Office has now provisioned a total of seven Federal Agencies on E3A.

Technical and sensitivity comments on the draft report have been provided under separate cover.

Following are our detailed responses to the four recommendations made by OIG.

Recommendation 1: Develop implementation measures and a delivery timeline to monitor progress of the E3A program.

Response: Concur

With respect to the implementation measures, the report references E3A Key Performance Parameters (KPPs) and states that the KPPs might not be useful or adequate performance measures. In addition, the report states these KPPs lack specific deliverables and milestones required to measure ISP status. Following DHS Management Directive 102 guidance, KPPs are designed to be high level system measures for the entire program and are not meant to be used as milestones or measures of a specific service provider. Measures for the delivery of Intrusion Prevention Security Services (IPSS) are detailed in contracts with IPSS service providers. In March of 2013 the National Cybersecurity Protection System (NCPS) Program Office identified performance measures to monitor the implementation of the IPSS services from the ISPs and included them in Statement of Objectives (SOOs) and Statements of Work (SOWs) provided to ISPs. Tailoring of those performance measures is discussed during Technical Exchange Meetings with ISPs and finalized throughout the contract negotiation process. Upon contract award, the final agreed to performance measures are written into the ISP contract and metrics captured for each is monitored monthly.

With respect to a delivery timeline to monitor the progress of E3A, there have been delays in contracting efforts due to the general readiness of the ISPs to meet the functional, security, and operational requirements of E3A. The contract action requires a certain amount of system design activities to be completed prior to contract award. This often requires a series of technical exchange meetings between the government and the ISP which adds time to the contracting effort. DHS has been actively engaged with the ISPs to work through DHS requirements and proposed ISP solutions since April 2012. In March 2013, the NCPS Program Office requested that each ISP provide a Service Delivery Plan (SDP) with their IPSS proposal. The SDP will outline the ISP's approach to meeting the full set of objectives and includes associated rough cost and schedule estimates. The information provided in the Service Delivery Plans is used to define out-year capability offerings.

Once contracts for a specific capability are awarded, the ISP creates a schedule for delivering capabilities that is submitted to the Government and monitored weekly for status updates. Weekly status meetings are held with each ISP to review progress toward the achievement of milestones. On a monthly basis, Program Management Reviews (PMRs) are conducted with

each ISP on contract to review overall cost and schedule performance for the contract and discuss risks and issues that are impacting the implementation of the capability. ISPs are also required to submit a Monthly Status Report (MSR) that details their progress toward meeting contractual requirements.

ECD: The development and implementation of performance measures was completed with Century Link (CTL) at the time of contract award (March 29, 2013). The process to define performance measures specific to contract activities prior to contract award will continue for all remaining ISPs. CTL's schedule for implementing DNS and Email services was submitted with their proposal and has been tracked weekly by the Program Office since that contract was awarded in March 2013. FY14, 4th Quarter, the NCPS Program Office will finalize the implementation schedule for IPSS.

Recommendation 2: Update training program to include the roles and responsibilities for the analyst to identify, minimize, and handle PII under E3A. A training schedule should be developed and offered periodically.

Response: Concur

DHS views privacy as more than just compliance with privacy laws. Privacy at DHS is also about public trust and confidence. It's about how the government acts responsibly and transparently in the way it collects, maintains, and uses personally identifiable information. DHS is committed to incorporating strong privacy and civil liberties protections into all cybersecurity activities. The NPPD Office of Privacy conducted Privacy Impact Assessments on its cybersecurity programs, including E3A to fully assess the privacy protections in place, ensuring those protections are based upon widely-accepted Fair Information Practice Principles.
DHS has taken a layered approach to protecting privacy of cybersecurity programs, to include working with US-CERT to establish standard operating procedures to ensure we minimize data collection to only information that is determined to be analytically relevant to pre-defined known or suspected cyber threats.

Prior to being released to the National Cybersecurity and Communications Integration Center (NCCIC) floor, the United States Computer Emergency Readiness Team (US-CERT) currently trains all US-CERT analysts (new hires) on its internal Standard Operating Procedures (SOPs). All US-CERT analysts are also trained on new or updated SOPs. SOPs for the handling of PII are included in the training and cover activities across US-CERT cyber capabilities or programs, including E3A. DHS reinforces privacy compliance through a separate oversight process to assess performance of the privacy requirements established through PIAs and privacy compliance reviews (PCR). In January 2012, DHS Privacy conducted a PCR on the EINSTEIN program. The PCR report is published on the DHS website: www.dhs.gov/privacy. In response to the recommendations from that review, the NPPD Office of Privacy developed and implemented a Quarterly Privacy Reviews (QPR) of PII handling to ensure that US-CERT is following their SOPs for the handling of PII; the first QPR was conducted October 2012.

US-CERT SOPs are considered living documents. As part of our ongoing efforts for oversight and compliance, US-CERT, in coordination with the NPPD Office of Privacy is in the process of

reviewing and updating US-CERT SOPs that address the handling of PII. SOPs are not meant to be "program specific" but rather cover activities across US-CERT capabilities and programs. As SOPs are updated, US-CERT will specifically identify those programs which are covered in its SOPs.

In addition, to supplement existing PII training, role-based training specific to PII handling is being developed by NPPD Office of Privacy, in coordination with US-CERT, and will be provided to all US-CERT analysts in addition to their current US-CERT SOP training. Role-based training will be required annually and conducted quarterly or as often as needed. Training will be scheduled and documented by the NCCIC Oversight and Compliance Officer.

ECD: FY14, 3rd Quarter, the NPPD Office of Privacy will have developed role-based training.

Recommendation 3: Revise the standard operating procedures to include specifications of current and subsequent E3A operational capabilities as well as analysts' roles and responsibilities for identification, minimization, and handling of PII under E3A.

Response: Concur

US-CERT SOPs are considered living documents; these SOPs define US-CERT analyst roles and responsibilities and cover activities across US-CERT cyber capabilities and programs. As part of its ongoing efforts US-CERT is continually in the process of reviewing and updating its internal SOPs, to include those that cover PII handling. SOPs are not meant to be "program specific" but rather cover activities across US-CERT capabilities and programs; however, as SOPs are updated, US-CERT will specifically identify those programs which are covered in each SOP.

ECD: FY14, 3rd Quarter, US-CERT will complete revisions to procedures covering E3A operational capabilities, including analyst roles and responsibilities regarding the identification and handling of PII.

Recommendation 4: Fix the identified vulnerabilities and out-of-compliance configuration settings on the Top Secret Mission Operating Environment or formally accept the residual risks for them in the appropriate Risk Management Matrix.

Response: Concur

The NCPS Program Office received an Authority to Operate the Top Secret Mission Operating Environment (TS MOE) on July 18, 2012 and the TS MOE follows the DHS Continuous Monitoring Strategy for assessing controls. As noted in the report, NPPD has implemented effective security controls on its TS MOE network and is 99.5 percent compliant with mitigations in place to ensure that they pose no direct or indirect threat vector to the network. The identified out-of-compliance configuration settings are minimal and are settings enabled as designed to allow for mission essential functionality to operate. At the time of the OIG audit, the Program Office informed the OIG that it intended to submit a DHS Information Security Program Request for Waivers and Exceptions to the accrediting authority to approve the

exception to configuration settings. The NCPS Program Office submitted the required DHS Information Security Program Request for Waivers and Exceptions for all findings to the accrediting authority on November 19, 2013. The exception request submitted states that while the configuration deviations exist, mitigations are in place to ensure that they pose no direct or indirect threat vector to the network.

ECD: Completed November 19, 2013

Again, we thank you for the opportunity to review and provide comment on this draft report, and we look forward to working with you on future engagements.

Sincerely,

Phyllis A. Schneck
Deputy Under Secretary for Cybersecurity

Appendix C
Major Contributors to This Report

Chiu-Tong Tsang, Director
Amanda Strickler, Lead IT Specialist
Shannon Frenyea, Program Analyst
David Bunning, IT Specialist
Sheldon Liggins, IT Auditor
Megan Ryno, Referencer
Michael Kim, Referencer

Appendix D
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Under Secretary, NPPD
Chief Information Officer, DHS
Chief Information Security Officer, DHS
Chief Information Officer, NPPD
Chief Information Security Officer, NPPD
Director, Compliance and Oversight, DHS OCISO
Chief Privacy Officer, DHS
Audit Liaison, CIO, DHS
Audit Liaison, CISO, DHS
Audit Liaison, NPPD

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov, or follow us on Twitter at: @dhsoig."

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Office of Investigations Hotline
245 Murray Drive, SW
Washington, DC 20528-0305

You may also call 1(800) 323-8603 or fax the complaint directly to us at (202) 254-4297.

The OIG seeks to protect the identity of each writer and caller.