The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

August 26, 2014

VIA ELECTRONIC MAIL

Brendan Goode, Director
National Protection and Programs Directorate
Office of Cybersecurity & Communications/Network Security Deployment
U.S. Department of Homeland Security
Arlington, VA 22201

Emily Andrew, Senior Privacy Officer
National Protection and Programs Directorate
Privacy Office
U.S. Department of Homeland Security
Arlington, VA 22209

RE: Privacy Compliance Review Follow-Up for the EINSTEIN Program

Dear Mr. Goode and Ms. Andrew:

The Department of Homeland Security (DHS) Privacy Office published a Privacy Compliance Review (PCR)[1] of the National Protection and Programs Directorate (NPPD) EINSTEIN Program[2] on January 3, 2012. The objective of the initial PCR was to assess compliance with the requirements in the EINSTEIN Privacy Impact Assessments (PIA).[3] The Privacy Office then conducted a follow-up PCR with the EINSTEIN program in 2014. The objective of the follow-up PCR was to determine the status of NPPD's implementation of the 2012 PCR recommendations. To achieve that objective, we reviewed the 2012 PCR recommendations and submitted written questions to the NPPD Privacy Office ("NPPD Privacy"). Privacy Office staff attended the NPPD Privacy and Office of Cybersecurity &

[1] The DHS Privacy Office conducts PCRs pursuant to its authority under Section 222 of the Homeland Security Act to assure that technologies sustain and do not erode privacy protections. Consistent with the Privacy Office's unique position as both an advisor and oversight body for the Department's privacy sensitive programs and systems, the PCR is designed as a constructive mechanism to improve a program's ability to comply with assurances made in existing privacy compliance documentation.

[2] EINSTEIN is a set of capabilities that are part of the overall National Cybersecurity Protection System (NCPS), managed by CS&C's Network Security Deployment (NSD) Division.

[3] U.S. Department of Homeland Security, Privacy Impact Assessment DHS/NPPD/PIA-001, The EINSTEIN Program, September 2004, http://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-einstein-june2013-3-year-review.pdf. U.S. Department of Homeland Security, Privacy Impact Assessment DHS/NPPD/PIA-008, EINSTEIN 2, May 19, 2008, http://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-einstein2-june2013-3-year-review.pdf.

Communications (CS&C) Quarterly Privacy Review on January 30, 2014. On June 30, 2014, Privacy Office staff met with NPPD Privacy to discuss their responses to the written questions.

This memorandum sets forth the Privacy Office's findings concerning the EINSTEIN program's compliance with the 2012 PCR Recommendations. The Privacy Office finds the EINSTEIN program compliant with these recommendations. I would like to thank the NPPD Privacy and CS&C staff for their support of this PCR and their responsiveness to our inquiries.

BACKGROUND

The Department of Homeland Security National Protection and Programs Directorate (NPPD) National Cyber Security Division (NCSD)[4] developed the EINSTEIN program in 2003 as a computer network intrusion detection system to help protect federal civilian executive agency information technology enterprises.[5] The Federal Government relies on its information technology (IT) infrastructure and the Internet to provide efficient and effective services to manage the growing amount of data needed to carry out its missions. This reliance makes the federal IT infrastructure a high-priority target for sophisticated adversaries.

EINSTEIN is a set of capabilities that have been deployed in phases: EINSTEIN 1, EINSTEIN 2, and EINSTEIN 3 Accelerated (E^3A). The EINSTEIN set of capabilities, which are part of the over-arching National Cybersecurity Protection System (NCPS),[6] are managed, deployed and maintained by Network Security Deployment (NSD) Division within the Office of Cybersecurity and Communications (CS&C). NCPS is an integrated system for intrusion detection, analysis, intrusion prevention, and information sharing capabilities that are used to defend the federal civilian government's information technology infrastructure from cyber threats.

The first phase, EINSTEIN 1, developed in 2003 serves as an automated process for collecting computer network security information from voluntary participating federal executive agencies. EINSTEIN 1 collects network flow records,[7] which identify the source Internet Protocol (IP) address of the computer that connects to the federal system; the port the source uses to communicate; the time the communication occurred; the federal destination IP address; the protocol used to communicate; and the destination port.

EINSTEIN 2, launched in 2008, incorporates an intrusion detection system capability that alerts when a pre-defined specific cyber threat is detected in federal network traffic. This

---

[4] In late 2012/early 2013, the Office of Cybersecurity and Communications reorganized and dissolved the National Cybersecurity Division. As a result of the reorganization, US-CERT was moved under the CS&C National Cybersecurity and Communications Integration Center. Network Security Deployment remained intact, reporting directly to CS&C.

[5] CS&C's Network Security Deployment (NSD) Division designs, develops, deploys, and sustains the National Cybersecurity Protection System (NCPS). NCPS capabilities support National Cybersecurity and Communications Integration Center (NCCIC)/United States Computer Emergency Readiness Team's operations and help prevent cyber-attacks on the .gov domain and/or reduce response/recovery time from cyber-attacks if they occur.

[6] U.S. Department of Homeland Security, Privacy Impact Assessment DHS/NPPD/PIA-026, National Cybersecurity Protection System, July 30, 2012, http://www.dhs.gov/sites/default/files/publications/privacy/privacy-pia-nppd-ncps.pdf.

[7] "Flow records" are records of connections made to a federal executive agency's IT systems.

provides the NCCIC/US-CERT with increased insight into the nature of that activity and gives them the ability to analyze cyber threat activity occurring across the participating federal IT networks resulting in improved computer network security situational awareness. This network intrusion detection technology uses a set of custom signatures[8] based upon known or suspected cyber threats. Each new level of EINSTEIN builds on the previous one, but EINSTEIN 1 and 2 continue to operate as distinct sets of capabilities as new EINSTEIN capabilities are introduced.

EINSTEIN 3 Accelerated (E^3A) is an intrusion prevention capability that allows DHS to not only detect malicious traffic, but also prevent it. This is accomplished by delivering intrusion prevention capabilities as a Managed Security Service (MSS)[9] that are provided by Internet Service Providers (ISPs) for intrusion prevention and threat-based decision making on network traffic entering or leaving the federal executive branch networks. When a signature alerts on known or suspected cyber threats, E^3A acts on that threat to prevent harm to the intended targets. Intrusion prevention improves DHS's ability to keep federal civilian networks secure.

NPPD conducted, and the Privacy Office reviewed and approved, PIAs for each EINSTEIN capability as well as for the NCPS, which is the overarching program covering all of the EINSTEIN capabilities. As NPPD looked ahead toward E^3A, the Privacy Office determined that conducting a PCR would be timely to ensure the accuracy of compliance documentation and the transparency of the EINSTEIN program moving forward.

The Privacy Office published a PCR of the EINSTEIN set of capabilities on January 3, 2012. The primary objective of the PCR was to assess the program's compliance with the EINSTEIN 2 (May 19, 2008) [10] and Initiative Exercise (March 18, 2010) PIAs.[11] The January 2012 PCR was completed before the launch of the new intrusion prevention program E^3A; therefore, E^3A was not included in that review.[12]

The initial PCR determined that the program had established privacy protections for EINSTEIN and was compliant with the PIAs' requirements concerning collection and use of information, internal sharing and external sharing with federal agencies, and accountability. The Privacy Office noted actions the program had taken to address retention and training requirements as outlined in the relevant EINSTEIN PIAs, but additional actions by the program were needed to bring it into full compliance with these requirements.

---

[8] Signatures are specific patterns of network traffic that affect the integrity, confidentiality, or availability of computer networks, systems, and information. For example, a specific signature might identify a known computer virus that is designed to delete files from a computer without authorization.

[9] MSS is a model by which the government articulates the objectives and services levels expected for their constituencies. MSS providers then determine how, where, when, and at what cost, those services will be delivered.

[10] See DHS/NPPD/PIA-008 EINSTEIN 2 (May 19, 2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf

[11] The Initiative 3 Exercise was an exercise relating to intrusion prevention capabilities. See DHS/NPPD/PIA-014 US-CERT: Initiative 3 Exercise (March 18, 2010) (RETIRED), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3.pdf.

[12] For a detailed description of the E^3A program, please see DHS/NPPD/PIA-027 EINSTEIN 3 Accelerated (April 19, 2013), *available at* http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/PIA%20NPPD%20E3A%2020130419%20FINAL%20signed.pdf.

In order to strengthen program oversight and external sharing, and to bring the program into full compliance with retention and training requirements, the Privacy Office recommended in the January 2012 PCR that:

1) the NPPD Privacy Office personnel be integrated into the signature review process and associated standard operating procedures (SOP), specifically that:

    a. NPPD senior privacy analyst is notified of all new signatures;

    b. NPPD senior privacy analyst reviews all templates for signatures targeting personally identifiable information (PII);

    c. NPPD senior privacy analyst is notified when PII is found and should establish a process to record the PII determination including retention of PII and the reasoning; and

2) the new compliance and oversight officer referenced in Standard Operating Procedure 110 conduct quarterly internal privacy reviews.

3) concerning external sharing,

    a. NCSD continue to work expeditiously to complete external sharing agreements with clauses outlining the sharing of PII; and

    b. NPPD Privacy Office review all information sharing memorandum of agreements.

4) NCSD complete a records schedule and submit it to the National Archives and Records Administration (NARA) for approval.

5) NCSD re-establish position-specific privacy training for all staff.

We conducted the current PCR to review the status of NPPD's implementation of these recommendations. Note that some of the office and program names have changed since the initial deployment of EINSTEIN and the initial PCR. CS&C is home to NCCIC/US-CERT and NSD, all referenced where appropriate below.

PCR FINDINGS

The Privacy Office finds CS&C compliant with the requirements outlined in the 2012 PCR. Our detailed findings are as follows:

1) Signatures

NPPD Privacy works closely with CS&C/NCCIC/US-CERT to ensure privacy is considered in the signature template and signature development process. The US-CERT 500-series SOPs describe the roles and responsibilities US-CERT must follow to develop and deploy signatures to detect malicious traffic within the EINSTEIN 2 environment. US-CERT analysts

must use the US-CERT EINSTEIN Management Signature Checklist (Checklist) when developing signatures. During the signature development process, if a signature contains PII, information that may be considered PII,[13] or is likely to capture PII, the signature package is sent to the NPPD Senior Privacy Analyst for review. After deployment of the signature, if PII is captured, the Senior Privacy Analyst, NCCIC Compliance and Oversight Officer, the DHS Office of General Counsel and Office of Civil Rights and Civil Liberties are notified and must determine whether the US-CERT justification for retaining the PII is sufficient.

The Senior Privacy Analyst is not notified of all new signatures, but only those that the US-CERT analyst marks (using the Checklist) as containing or likely to capture PII or information that may be considered PII. During Quarterly Privacy Reviews (QPR), the NPPD Senior Privacy Analyst reviews a sampling of all of the signatures developed, whether or not they were marked to include PII (see next section).

After discussing the signature review process with NPPD Privacy and reviewing sample signatures and notifications, the Privacy Office finds that NPPD Privacy is sufficiently involved in the signature development process to ensure PII is not unnecessarily used, captured, or retained during EINSTEIN processes.

2) Quarterly Privacy Reviews

NPPD Privacy holds QPRs concerning PII handling within CS&C. Privacy Office staff attended the QPR on January 30, 2014. In preparation for the QPRs, the NPPD Senior Privacy Analyst reviews signatures developed during the quarter to ensure that PII, either included in the signature or captured by the signature, has been handled properly. Initially, the Senior Privacy Analyst reviewed all of the signatures developed during a quarter. Through January 2014, the Senior Privacy Analyst reviewed a total of 942 signatures over six quarters, and approximately 2.5% of those signatures included or captured PII. In light of the large number of signatures, US-CERT's consistent compliance with the Checklist, and referral of signatures with PII to the Senior Privacy Analyst for approval, NPPD Privacy determined during the January 2014 QPR that reviewing a random sample of signatures each quarter provides adequate oversight. During the May 2014 QPR, the Senior Privacy Analyst reviewed a random sample of 205 signatures out of a total of 304 signatures developed during the quarter. NPPD Privacy will continue to review random samples of signatures during subsequent QPRs.

NPPD Privacy provides a quarterly PII Retention Deletion Memo to provide specific recommendations to US-CERT for handling signatures identified during the quarter that contain PII. NPPD Privacy and CS&C staff also discuss other matters such as updates to SOPs and compliance with privacy procedures. NPPD Privacy distributes a final report summarizing the QPR review and any recommendations and action items.

The Privacy Office reviewed the signature review documentation and QPR final reports. The Privacy Office finds that the quarterly reviews provide regular opportunities for NPPD

[13] "Information that may be considered PII" refers to certain indicators of a cyber threat that can be the same type of information individuals use to identify themselves in online communications, such as email address or an IP address and domain information.

Privacy to verify that PII is being handled appropriately and to assist in refining procedures to implement the most effective privacy protections for the EINSTEIN program.

3) External Sharing Agreements

NPPD Privacy contributed to developing a Memorandum of Agreement (MOA) template for use in providing EINSTEIN services to participating federal departments and agencies. NSD does not provide EINSTEIN services to any agency without a signed MOA. The most recent MOA template covers all three EINSTEIN services. As agencies sign the new MOA, previously executed EINSTEIN MOAs will be retired. NSD, in conjunction with NPPD Privacy and the DHS Office of General Counsel drafted the MOA and appendices (Model Language for Long-On Banners for Computers, Model Language for User Agreement, and Model Language for Privacy Policy). NPPD Privacy also coordinated with the Privacy Office, and the Chief Privacy Officer approved the template. NSD is required to use the MOA template; therefore, NPPD Privacy does not review every MOA. If an MOA needs to be edited for a particular agency in a way that would affect the privacy provisions, NPPD Privacy would review the MOA before it is approved, but this has not yet occurred. As NPPD Privacy was heavily involved in the development of the MOA template, the Privacy Office is satisfied that reviewing new MOAs individually is not necessary.

The Privacy Office reviewed the MOA template, appendices, and inventory of existing MOAs and finds that they provide for the protection of PII when NSD shares EINSTEIN information with other federal agencies.

4) Records Retention Schedule

The National Cybersecurity Protection System (NCPS) records schedule has been completed and is currently with NARA awaiting approval.

5) Position-Specific Privacy Training

NPPD Privacy developed position-specific privacy training for CS&C analysts and Senior Watch Officers. The CS&C Cyber Threat Privacy Training was developed specifically to address proper handling of PII as articulated in the US-CERT Cybersecurity Information Handling Guidelines. This training has been delivered to a group of US-CERT analysts, and NPPD Privacy will revise the training materials on an ongoing basis as updates to the SOPs or other procedures are implemented. NPPD Privacy also developed privacy training specific to CS&C Senior Watch Officers who support cyber activities on the NCCIC Watch Floor. The Privacy Office reviewed these training materials and finds that they create a strong foundation for privacy protection within cybersecurity programs.

RECOMMENDATIONS

We recognize that the NSD and NCCIC/US-CERT have many robust privacy protections in place to address privacy concerns related to EINSTEIN capabilities, and commend CS&C and NPPD Privacy for their responsiveness to the 2012 PCR recommendations. I am pleased that NPPD Privacy has fully implemented the CS&C Cyber Threat Privacy Training. The Privacy Office has no recommendations at this time.

NCPS and its EINSTEIN capabilities are the subject of various oversight bodies and the program recently underwent an extremely thorough review by the DHS Office of Inspector General. I appreciate NPPD Privacy and CS&C's cooperation with us during our review Please direct any questions regarding this PCR and its results to Jonathan Cantor, Deputy Chief Privacy Officer.

Sincerely,

Karen L. Neuman
Chief Privacy Officer

cc: Dr. Andy Ozment, Assistant Secretary of CS&C