Privacy Compliance Review

of the

EINSTEIN Program

January 3, 2012

Contact Point
Brendan Goode
Director, Network Security Deployment
National Protection and Programs Directorate
(703) 235-2853

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

I. SUMMARY

The Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) National Cyber Security Division (NCSD) launched the EINSTEIN program in 2004 as a computer network intrusion detection system to help protect federal executive agency information technology enterprises. NCSD deployed EINSTEIN in phases including EINSTEIN 1, EINSTEIN 2, and the Initiative 3 Exercise (Exercise), with each phase adding new functionality.

The first phase, EINSTEIN 1 was launched in 2004 and serves as an automated process for collecting computer network security information from voluntarily participating federal executive agencies. EINSTEIN 1 collects network flow records,[1] 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 network intrusion detection that monitors for malicious activity in network traffic to and from participating federal executive agencies. This gives the United States Computer Emergency Readiness Team (US-CERT)[2] the ability to analyze malicious activity occurring across the federal IT networks resulting in improved computer network security into the basic platform of the EINSTEIN program capabilities. This network intrusion detection technology uses a set of custom signatures[3] based upon known malicious network traffic. Each new level of EINSTEIN builds on the previous one but EINSTEIN 1 and 2 continue to operate as distinct programs as new capabilities are introduced to later versions.

In 2010, NCSD launched the Exercise to identify the ability of an existing Internet Service Provider to select and redirect internet traffic from a single participating government agency through the Exercise technology. The Exercise applied intrusion detection and prevention measures to that traffic and allowed for US-CERT to generate automated alerts about selected cyber threats. As the EINSTEIN program progresses EINSTEIN 1, 2 and eventually 3 will continue to work to prevent cyber threats from attacking the federal system and increase cybersecurity.

NCSD conducted Privacy Impact Assessments (PIAs) for each phase of the EINSTEIN program, which the DHS Privacy Office reviewed and approved. As NCSD looks ahead toward the next phase of the program to EINSTEIN 3, the DHS Privacy Office

[1] "Flow records" are records of connections made to a federal executive agency's IT systems.
[2] US-CERT is the operational arm of the National Cyber Security Division (NCSD) at the Department of Homeland Security (DHS). US-CERT's mission is to improve the nation's cybersecurity posture, coordinate cyber information sharing and proactively manage cyber risks to the nation while protecting the constitutional rights of Americans.
[3] 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.

determined that conducting a Privacy Compliance Review (PCR) would be timely to ensure the accuracy of compliance documentation and transparency of the EINSTEIN program moving forward.[4]

The primary objective of the PCR was to assess NCSD's compliance with existing privacy compliance documentation, specifically the EINSTEIN 2 (May 19, 2008) and Initiative 3 Exercise (March 18, 2010) PIAs.[5] To address our objective, the DHS Privacy Office reviewed Standard Operating Procedures (SOPs), Concept of Operations for National Cybersecurity Protection System (NCPS) – which includes EINSTEIN capabilities, international agreements, and signature templates. The DHS Privacy Office also held a question and answer session with NPPD/NCSD leadership, conducted two visits of the US-CERT analyst site, and interviewed US-CERT analysts who use, have access to, and are responsible for the accuracy of EINSTEIN program capabilities.

The review was conducted from May to July 2011 and was led by the DHS and NPPD Privacy Offices. Throughout the review, the DHS Privacy Office collaborated with the leadership of NPPD and NCSD including the: former US-CERT Director; Acting US-CERT Director; US-CERT Deputy Chief of Operations; Network Security Deployment, System Sustainment and Operations Section Chief; and Director, Network Security Deployment. NPPD/NCSD recently hired a senior privacy analyst to work on privacy protections and issues for the EINSTEIN program. This review occurred before the analyst could be fully integrated into the general practices of NCSD.

II. FINDINGS

The DHS Privacy Office found NPPD/NCSD generally compliant with the requirements outlined in the EINSTEIN 2 PIA and Initiative 3 Exercise PIA. Specifically, NPPD/NCSD is fully compliant on collection of information, use of information, internal sharing and external sharing with federal agencies, and accountability requirements. The DHS Privacy Office identified actions taken to address retention and training requirements as outlined in the relevant EINSTEIN PIAs, but additional actions by the program are needed to bring them into full compliance with these requirements. The DHS Privacy Office is making five recommendations to strengthen program oversight, external sharing, and bring NPPD/NCSD into full compliance with retention and training requirements. NPPD agreed with our findings and is taking steps to address our recommendations.

[4] The DHS Privacy Office exercises its authority under Section 222 of the Homeland Security Act to assure that technologies sustain and do not erode privacy protections through the conduct of PCRs. Consistent with PRIV's unique position as both and 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.

[5] See EINSTEIN 2: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf and Initiative 3 Exercise: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3.pdf.

III. PRIVACY COMPLIANCE REVIEW

Signatures

Requirements from the EINSTEIN 2 PIA and the Initiative 3 Exercise PIA: Signatures, as defined, 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.

NPPD/NCSD follows a specific process to create each signature so it only focuses on a specific cyber threat. The signatures are subject to review by the Office of General Counsel, the Oversight and Compliance Office of US-CERT, as well as the DHS and NPPD Privacy Offices. US-CERT deploys signatures that use Personally Identifiable Information (PII) only if the signatures have been approved in accordance with written procedures and only for the purpose of detecting cyber threats. If a deployed signature captures more network traffic than is necessary or relevant to understand a cyber threat, that signature is considered to be failing, and will be reviewed and modified or removed, thus further limiting the amount of data US-CERT analysts receive.

Review: PRIV reviewed the process used to create signatures. The DHS Privacy Office reviewed a sample of signatures, all the templates used to create signatures, and all the signatures that target PII. The DHS Privacy Office reviewed the procedures for a failing signature including rewriting or deleting the signature when necessary. The DHS Privacy Office also interviewed US-CERT analysts who create signatures and run signatures through the EINSTEIN program capabilities.

Finding: The DHS Privacy Office found NPPD/NCSD to be in compliance with the requirements outlined in the EINSTEIN 2 PIA and Initiative 3 Exercise PIA. NPPD/NCSD, through signatures, does not collect more PII than necessary to detect cyber threats and when extraneous PII is collected, it is removed completely and quickly.

Recommendation: To ensure a more accountable signature process, the DHS Privacy Office recommends inclusion of the NPPD Privacy Office along with the DHS Privacy Office in the review of templates for types of signatures that could contain PII.

Collection of Information

Requirements from the EINSTEIN 2 PIA and the Initiative 3 Exercise PIA: EINSTEIN 2 and the Exercise observe Internet traffic from the federal executive branch and deploy signatures and alerts on suspected cyber threats. Information is collected only when it relates to a specific cyber threat and only when a signature signals that the information is a match to a known or suspected cyber threat. US-CERT reviews and processes the data in accordance with its written information handling procedures. The procedures, as outlined in the PIAs, state that US-CERT personnel must determine if PII collected is necessary for subsequent US-CERT analysis in furtherance of its network security

activities and protection of federal systems before such data is further processed or retained. Information deemed unnecessary for subsequent US-CERT analysis is purged. When PII is required for analysis, the US-CERT personnel will log the need and report the use of PII to the US-CERT director and the oversight and compliance officer.

Review: NPPD/NCSD did collect PII during the operations of EINSTEIN 2 but not during the Initiative 3 Exercise. The PII included email header and the body of the email message and its collection was the result of one signature targeting a known cyber threat. The DHS Privacy Office interviewed US-CERT analysts about their handling practices regarding this signature. In addition, the DHS Privacy Office reviewed SOP 108 – Identifying Sensitive Information: PII Handling and Minimization and SOP 110 – PII Handling and Minimization to determine if appropriate procedures were in place to ensure that PII is retained only when reasonably necessary and under sufficient protections.

Finding: The DHS Privacy Office found NPPD/NCSD in compliance with the requirements and procedures outlined in the EINSTEIN 2 PIA and Initiative 3 Exercise PIA. For example, for PII collected during the operation of EINSTEIN 2, US-CERT analysts reviewed the PII to determine its link to a known cyber threat and then deleted it in accordance with SOP 108. Further, SOP 108 and SOP 110 provide adequate procedures to ensure PII is retained only when reasonably necessary and under sufficient protections. SOP 108 details accurately labeling the PII, requiring encryption and limiting dissemination of the PII to only those necessary for further analysis. Additionally, SOP 110 requires reporting the retention of PII through the US-CERT chain of command and to the oversight and compliance officer.

Recommendation: To strengthen these procedures, the DHS Privacy Office recommends NPPD/NCSD update SOP 108 and 110 to reference the newly appointed NPPD/NCSD senior privacy analyst. This update should include quarterly reviews by the NPPD/NCSD senior privacy analyst of any PII retained, including descriptions of why it is necessary to retain the PII and a process to verify deletion. This update is currently in progress.

Use of Information

Requirements from the EINSTEIN 2 PIA and the Initiative 3 Exercise PIA: NPPD/NCSD views Internet traffic for the federal executive branch for the following specific uses: 1) to identify cyber threats or 2) notify another agency that it may have a cyber threat. When NPPD/NCSD identifies a cyber threat, it issues a report to the specific agency that has a cyber threat or to the entire federal executive branch. The reports are only handled by trained and experienced computer network security professionals subject to oversight and audits.

Review: The DHS Privacy Office interviewed US-CERT analysts and reviewed their procedures for issuing reports to other agencies about cyber threats. The DHS Privacy Office also reviewed a sample of the reports issued to other agencies.

Finding: The DHS Privacy Office found NPPD/NCSD to be in compliance with the requirements outlined in the EINSTEIN 2 PIA and Initiative 3 Exercise PIA.

Retention of Information

Requirements from the EINSTEIN 2 PIA and the Initiative 3 Exercise PIA: A retention schedule and disposal policy for this initiative needs to be established and approved by the NPPD records officer and the National Archives and Records Administration (NARA). Any information collected related to a cyber threat will be maintained for up to three years.

Review: The DHS Privacy Office interviewed NPPD/NCSD and NPPD Privacy officials to identify retention practices and whether a records retention schedule had been established and approved by the NPPD records officer and NARA.

Finding: NPPD/NCSD follows a draft records retention schedule and a disposal policy that has been prepared but has not yet been submitted to NARA for approval. Current practice from NPPD/NCSD calls for storing operational data for only six months and archival data for no more than three years but usually for a shorter period.

Recommendation: To fully establish these procedures, the DHS Privacy Office is recommending that NPPD/NCSD finalize their records schedules and submit to NARA for approval. NCSD is currently working with NPPD Privacy to finalize its records schedules and submit for approval to NARA.

Internal and External Sharing and Disclosure

Requirements from the EINSTEIN 2 PIA and the Initiative 3 Exercise PIA: NPPD/NCSD only shares information in the form of reports regarding specific cyber threats. These reports are shared internally within DHS in furtherance of the DHS cybersecurity mission. The reports are designed to minimize any PII found and only report on specific cyber threats.

External sharing through reports requires an executed Memorandum of Agreement (MOA) between NPPD/NCSD and the agency or other organization before any information can be shared.

Review: The DHS Privacy Office interviewed NPPD/NCSD officials and reviewed SOPs to identify internal and external sharing practices. The DHS Privacy Office also reviewed several MOAs in place between NPPD/NCSD and external agencies which included two international sharing agreements (Israel and India).

Finding: The DHS Privacy Office found NPPD/NCSD to be compliant with internal sharing and external sharing requirements. Internal sharing consists of reports sent by

NPPD/NCSD to DHS components. NPPD/NCSD has information handling SOPs in place that direct this sharing and ensure compliance. External sharing involves US-CERT providing reports to U.S. federal government agencies regarding possible threats to their systems. Federal agencies in return report possible cyber threats to their network to NPPD/NCSD to ensure broad knowledge of the threat is available. Before the reports are shared, an MOA is completed which outlines what information the reports contain regarding the cyber threats and the limits on sharing. The MOAs the DHS Privacy Office reviewed contain guidance on how to work with NCSD and outline of the specific roles of DHS and the partner agency.

During the Exercise, external sharing was limited to within the federal government but currently, US-CERT collaborates with foreign governments through the use of EINSTEIN 2 technology. US-CERT analysts share reports with international partners but the DHS Privacy Office found no SOPs outlining what information to share and what to withhold. The DHS Privacy Office requested any relevant information sharing agreements, and was provided with two MOAs (Israel and India). The DHS Privacy Office reviewed these agreements and found no restrictions or guidelines on sharing information like PII. External sharing internationally was not directly mentioned in the PIAs and US-CERT was unaware of the DHS Privacy Office's concerns.

Recommendations: Moving forward, the DHS Privacy Office recommends that US-CERT require a provision describing what PII is to be shared in the reports and retention rates in MOAs with all foreign partners. This should be done in consultation with the DHS Privacy Office and the DHS Office of International Affairs. Additionally, the DHS Privacy Office recommends that these reports be reviewed annually by the NPPD Privacy Office to ensure compliance and SOPs should be circulated to the US-CERT analysts so they are aware what information should and should not be shared with international partners.

Training and Accountability

Requirements from the EINSTEIN 2 PIA and the Initiative 3 Exercise PIA: NPPD/NCSD must provide privacy training for all analysts on an annual basis and on specific privacy issues related to the US-CERT's computer network defense responsibilities.

US-CERT must create procedures to ensure all data is handled correctly and in a secure manner. US-CERT will analyze the data collected in accordance with its written information handling procedures as outlined in its Standard Operating Procedures.

Review: The DHS Privacy Office interviewed NPPD/NCSD officials to identify privacy training and oversight practices. The DHS Privacy Office also reviewed information handling SOPs to identify accountability measures in place.

Finding: NPPD/NCSD provided initial privacy training on a quarterly basis but has not kept up with new staff or annual training for experienced staff. Currently, new staff and experienced staff receive basic DHS-wide privacy training but have not received privacy

training specific to the work at NPPD/NCSD since the former compliance officer vacated his position in November 2010. The new compliance officer started in May 2011. NPPD/NCSD has hired a senior privacy analyst and a compliance and oversight officer to resume the specific privacy training required in the PIAs. Additionally, the SOPs outline the need for additional privacy training and list specific requirements to be met. The DHS Privacy Office is recommending that NPPD/NCSD re-establish position-specific privacy training for all staff. NPPD/NCSD understands the need to develop privacy training specific to the EINSTEIN program and is working aggressively to accomplish that goal.

The DHS Privacy Office found NPPD/NCSD compliant on accountability requirements. Specifically, standard operating procedures such as SOP 445, which describe the process to obtain more detailed information on a known malicious IP address, were thorough and accounted for handling of PII. In addition, SOP 110 requires quarterly internal reviews to evaluate and assess compliance with NPPD/NCSD's information handling procedures. NPPD/NCSD recently hired a compliance and oversight officer to perform internal audits and compliance with SOPs.

Recommendations: The DHS Privacy Office is making several recommendations to improve NPPD/NCSD oversight. Specifically, the DHS Privacy Office recommends that the new compliance and oversight officer undertake the quarterly internal reviews referenced in SOP 110. Additionally, the DHS Privacy Office recommends amending SOP 445 and SOP 110 to include the NPPD/NCSD senior privacy analyst in reviews of the data handling procedures to ensure accountability. For example, if PII is encountered during the analysis process, the analyst is told to refer to SOP 108 and report the incident to the US-CERT supervisor. Finally, the DHS Privacy Office recommends that in addition to referencing SOP 108, the NPPD/NCSD senior privacy analyst receives a report on the PII as well.

IV. CONCLUSION AND RECOMMENDATIONS

NPPD/NCSD has worked hard to establish privacy protections for the EINSTEIN program as evidenced by our finding that NPPD/NCSD is generally compliant with the requirements outlined in the EINSTEIN 2 PIA and Initiative 3 Exercise PIA. Specifically, NPPD/NCSD is fully compliant on collection of information, use of information, internal sharing and external sharing with federal agencies, and accountability. The DHS Privacy Office identified actions taken to address retention and training requirements as outlined in the relevant EINSTEIN PIAs, but additional actions by the program are needed to bring them into full compliance with these requirements. The DHS Privacy Office is making five recommendations to strengthen program oversight, external sharing, and bring NPPD/NCSD into full compliance with retention and training requirements. The DHS Privacy Office recommends:

1. integration of the NPPD Privacy Office personnel into the signature review process and associated SOPs, specifically:
    a. NPPD/NCSD senior privacy analyst is to be notified of all new signatures;
    b. NPPD/NCSD senior privacy analyst is to review all templates for signatures targeting PII;
    c. NPPD/NCSD senior privacy analyst is to be notified when PII is found and should establish a process to record the PII determination including retention of PII and the reasoning; and
    d. NPPD Privacy Office is to review all information sharing memorandum of agreements.
2. Quarterly internal reviews by the new compliance and oversight officer referenced in SOP 110.
3. NPPD/NCSD continue to work expeditiously to complete external sharing agreements with clauses outlining the sharing of PII.
4. Complete the NPPD/NCSD records schedules and submit to NARA for approval.
5. NPPD/NSCD re-establish position-specific privacy training for all staff.

NPPD is currently taking steps to address these recommendations. At the next PCR, which will occur in the fall of 2013, the DHS Privacy Office will review the measures taken to implement these recommendations and the progress of the program.

V. PRIVACY COMPLIANCE REVIEW APPROVAL

Responsible Official

Brendan Goode
Director, Network Security Deployment
National Protection and Programs Directorate

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security