Privacy Compliance Review
of the
Enhanced Cybersecurity Services (ECS) Program

April 10, 2015

Contact Point
Andy Ozment
Cybersecurity and Communications
National Protection and Programs Directorate
(703) 235-5999

Emily Andrew
Senior Privacy Officer
National Protection and Programs Directorate
(703)-235-2182

Reviewing Official
Karen Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Table of Contents

I. Background

Enhanced Cybersecurity Services (ECS) is a voluntary Department of Homeland Security (DHS) program in which the National Protection and Programs Directorate's (NPPD) Cybersecurity and Communications (CS&C)[1] provides indicators of malicious cyber activity[2] to participating commercial service providers (CSPs).[3] An indicator is human-readable cyber data (e.g., related to Internet Protocol (IP) addresses, domains, e-mail headers, files, and strings) used to identify some form of malicious cyber activity.[4] These indicators can be used to create intrusion detection signatures[5] or other means of detecting and mitigating cyber threats. The purpose of the program is to assist the owners and operators of critical infrastructure[6] in enhancing their ability to protect their systems from unauthorized access, exploitation, or data exfiltration through a voluntary information sharing program.

Under the program, DHS/NPPD/CS&C identifies cybersecurity indicators that are crucial for protecting critical infrastructure and shares that information with CSPs through secure communication channels. The CSPs may then configure the indicators into "signatures," which are machine-readable software code that enable the automated detection of the known or suspected cyber threats associated with the indicators.[7] Owners and operators in recognized critical infrastructure sectors[8] may enter into commercial agreements with CSPs to receive

[1] Although the PIA references NPPD/CS&C as having responsibility for ECS, NPPD/CS&C's cyber operations have gone through reorganization, and responsibility for ECS now falls under Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR). All references in the PIA and the PCR may be interpreted to apply to SECIR after the reorganization.

[2] Cyber threats can be defined as any identified efforts directed toward accessing, exfiltrating, manipulating, or impairing the integrity, confidentiality, security, or availability of data, an application, or a federal system, without lawful authority. Information about cyber threats may be received from government, public, or private sources. Categories of cyber threats may include, for example; phishing, IP spoofing, botnets, denials of service, distributed denials of service, man-in-the-middle attacks, or the insertion of other types of malware.

[3] The ECS Program is also open to "operational implementers," which are critical infrastructure entities that wish to deploy ECS on their own networks and do not wish to contract with a CSP to do so. The requirements for operational implementers are the same as those for CSPs. For simplicity, references in the PCR to CSPs also apply to operational implementers.

[4] Indicators can be either unclassified or classified. Whether an indicator is classified is dictated by its source.

[5] Signatures are specific machine-readable 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.

[6] "Critical infrastructure" refers to the assets, systems, and networks, whether physical or virtual, that are so vital to the United States that their incapacitation or destruction would have a debilitating effect on physical and national economic security, public health or safety, or any combination thereof.

[7] Additional information about indicators and signatures is addressed in the National Cybersecurity Protection System (NCPS) Privacy Impact Assessment, published July 30, 2012 and available at: http://www.dhs.gov/sites/default/files/publications/privacy/privacy-pia-nppd-ncps.pdf.

[8] Homeland Security Presidential Directive 7 (HSPD-7) identifies 17 critical infrastructure sectors, and allows for DHS to identify gaps in existing sectors and establish new sectors to fill these gaps. Under this authority, DHS designated Critical Manufacturing as an 18th sector in March 2008. In February 2013, Presidential Policy Directive 21 designated 16 critical infrastructure sectors. A future update of the ECS PIA will reflect the current 16 sectors.

cybersecurity protections based on the signatures developed by the CSPs from indicators received through ECS. DHS is not a party to the agreements between the CSPs and critical infrastructure owners and operators.

NPPD conducted a Privacy Impact Assessment (PIA) of ECS in January 2013,[9] which the DHS Privacy Office reviewed and approved. Additionally, the DHS Privacy Office reviewed the privacy risks and impacts associated with the program as part of the Executive Order 13636[10] Privacy and Civil Liberties Assessment Report completed in April 2014. As part of its Executive Order 13636 assessment, DHS committed "to conduct an in-depth Privacy Compliance Review [PCR] of the entire ECS Program in 2014" and to "report the results in the 2015 annual report required by [Executive Order] 13636."[11] Accordingly, the DHS Privacy Office conducted a PCR[12] of ECS with the primary objective of assessing the program's compliance with the existing PIA.

To fulfill this objective, the DHS Privacy Office reviewed policies and standard operating procedures for the ECS Program; internal correspondence, technical/process documentation, use cases, and decision memoranda regarding new program services; monthly performance reporting; and information sharing agreements.

ECS is an information sharing program that shares cybersecurity indicators. These indicators may be received through other DHS cybersecurity programs or processes referenced in the ECS PIA, such as those related to EINSTEIN or performed by the United States Computer Emergency Readiness Team (US-CERT). To conduct a full PCR of ECS, the DHS Privacy Office also reviewed cybersecurity indicator development and processing that occurs through other DHS cybersecurity programs or processes, if those programs or processes are referenced or described in the ECS PIA. This review of related topics described in the PIA included: sample signatures developed from indicators; National Cybersecurity Protection System (NCPS) system access, use, and incident response; quarterly privacy reviews of the handling of personally identifiable information (PII); US-CERT cybersecurity information handling procedures and training; records retention; and indicator verification and vetting. The PCR was conducted from July to October 2014 and was led by the DHS Privacy Office, in coordination with the NPPD Office of Privacy and CS&C.

---

[9] *See* DHS/NPPD/PIA-028 Enhanced Cybersecurity Services, January 16, 2013. Available at: http://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_nppd_ecs_jan2013.pdf.

[10] Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," February 12, 2013. 78 Fed. Reg. 11739. Available at: http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

[11] *See* "Executive Order 13636 Privacy and Civil Liberties Assessment Report," April 2014. Available at: http://www.dhs.gov/sites/default/files/publications/2014-privacy-and-civil-liberties-assessment-report.pdf.

[12] In conducing PCRs, 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. Consistent with the DHS 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.

Because ECS shares indicators that may be received through other DHS cybersecurity programs or processes, this PCR builds upon previous PCRs conducted on DHS cybersecurity activities that may be referenced or described in the ECS PIA. Specifically, DHS published a PCR of the EINSTEIN program on January 3, 2012.[13] On August 26, 2014, DHS also published a follow-up report on implementation of the 2012 EINSTEIN PCR recommendations.[14]

II. Scope and Methodology

The DHS Privacy Office conducted a PCR of the ECS Program, in coordination with NPPD/CS&C and the NPPD Office of Privacy, for the activity period of January 2013 through September 2014. ECS is a program that shares cybersecurity indicators that are received by DHS through other DHS programs or processes. Therefore, to obtain a comprehensive understanding of ECS in the larger DHS cyber programmatic environment, the DHS Privacy Office also reviewed cybersecurity indicator development and processing that occurs through other DHS programs or processes if those programs or processes are referenced or described in the ECS PIA. To assess ECS' overall compliance with the current PIA, the DHS Privacy Office carried out the following activities:

- Reviewed the current PIA.
- Developed and administered a questionnaire to NPPD that included questions about:
  - compliance with the DHS Fair Information Practice Principles;
  - indicator development, review, and maintenance;
  - cyber information sharing; and
  - access controls, security, and auditing.
- Conducted follow-up engagement with NPPD on its responses to the questionnaire.
- Reviewed a variety of documentation specific to the ECS Program, including:
  - policies and standard operating procedures;
  - internal correspondence, technical/process documentation, use cases, and decision memoranda regarding new program services;
  - monthly performance reporting; and
  - Memorandum of Agreement (MOA) templates.
- Reviewed a variety of documentation related to activities that occur outside of the ECS Program but are necessary for its operation and are referenced or described in the ECS PIA, including:
  - sample signatures, developed from indicators;

[13] *See* "Privacy Compliance Review of the EINSTEIN Program," January 3, 2012. Available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_privcomrev_nppd_ein.pdf.
[14] *See* Letter from Karen L. Neuman to Brendan Goode and Emily Andrew, "Privacy Compliance Review Follow-Up for the EINSTEIN Program," August 26, 2014. Available at: http://www.dhs.gov/sites/default/files/publications/einstein%20pcr%20ltr%20august%202014.pdf.

- NCPS system access, use, and incident response;
- quarterly privacy reviews of the handling of PII; and
- US-CERT cybersecurity information handling procedures and training; records retention; and indicator verification and vetting.

In developing this report, the DHS Privacy Office followed a four-step template for each subsection below. The template includes: (1) a description of the requirements from the ECS PIA, which are derived from the DHS Fair Information Practice Principles, the Department's framework for analyzing the privacy impacts of all DHS programs; (2) our review of the requirements; (3) the results of our review of the requirements; and (4) our findings and recommendations, if applicable.

III. Findings

A. Summary

The DHS Privacy Office finds that NPPD developed the ECS Program and its related processes with privacy-protective objectives in mind. NPPD continues to operate the ECS Program and its related processes with strong privacy oversight, which allows NPPD to identify and mitigate privacy risks as the program evolves and matures.

As a result of NPPD's excellent privacy-by-design, our recommendations are limited to updates that should be made to the ECS PIA to augment NPPD's already robust transparency and address changes in the program as it has matured. Detailed recommendations are included in the analysis sections below and listed in the conclusion (see Section IV). Each recommendation is preceded by a discussion of the ECS privacy requirements as set out in the ECS PIA and the DHS Fair Information Practice Principles.

NPPD indicated that as part of its normal business processes it will be updating the ECS PIA in the event that any new ECS services are offered. The DHS Privacy Office looks forward to the inclusion of the updates recommended in this report in such a future ECS PIA update.

B. Cybersecurity Indicators

1. Identifying, Minimizing, and Marking PII

ECS PIA Requirements:

The PIA permits NPPD/CS&C to share indicators that may contain information that could be considered PII[15] with CSPs. Information that could be considered PII may be part of e-mail-related indicators, such as the sender's name or e-mail address; information from and associated with e-mail messages; and other information that could be contained in the message header, such as to/from free-flow text fields or subject line from individuals.

However, NPPD/CS&C will review and retain this information only if that information is analytically relevant to understanding the cyber threat. In other words, information that could be considered PII will only be shared with CSPs if the PII is reviewed by NPPD/CS&C and determined to be an indicator of a known or suspected cyber threat.

NPPD/CS&C will follow defined standard operating procedures for identifying and handling information that could be considered PII (e.g., overwriting, redacting, or replacing PII), as well as its cybersecurity information handling guidelines, to minimize the inclusion of information that could be considered PII in indicators.

Review:

NPPD/CS&C only shares indicators that are reviewed by US-CERT analysts. Accordingly, the DHS Privacy Office reviewed a written response from NPPD/CS&C describing the US-CERT processes for handling indicators that contain information that could be considered PII. The DHS Privacy Office also conducted follow-up engagement with NPPD based on NPPD's written response.

The DHS Privacy Office also reviewed the US-CERT Cybersecurity Information Handling Guidelines and US-CERT standard operating procedures addressing identifying sensitive information, including PII; handling and minimizing PII; and addressing non-cyber PII. The DHS Privacy Office also reviewed the results of Quarterly Privacy Reviews from the fourth quarter of fiscal year 2012 to the third quarter of fiscal year 2014, which are NPPD's internal reviews of the handling of PII at NPPD/CS&C. The DHS Privacy Office also reviewed a sample

[15] DHS uses the phrase "information that could be considered PII" because certain indicators of a cyber threat can be the same type of information individuals use to identify themselves in online communications, such as an e-mail address or other information that might be included in the message or subject line. In the context of CS&C programs and processes, and the subsequent analysis, these types of information are generally not used to identify an individual; instead, they are used as a reference point for particular known or suspected cyber threats.

of seven signatures.[16] These signatures were based on indicators that contain information that could be considered PII, as well as the NPPD Senior Privacy Analyst's assessment of the signatures.

Results of Review:

NPPD has appropriate procedures to identify, minimize, and mark indicators that contain information that could be considered PII.

US-CERT analysts follow standard operating procedures to identify PII. These procedures require analysts to screen all data and information received from any source in any format to determine whether the information contains PII. Once PII is identified, analysts are required to review and redact PII unless it is "necessary" for US-CERT analysis to protect an information system from cybersecurity threats, mitigate against such threats, or respond to a cybersecurity incident. In determining whether PII is necessary for US-CERT analysis, US-CERT's Cybersecurity Information Handling Guidelines specify that analysts may consider, for example, whether the information relates to a known or suspected cybersecurity threat or cyber incident; will be necessary to understand subsequent US-CERT products; otherwise enables victim identification; enhances threat mitigation; or improves insight into other known or suspected cybersecurity threats or cyber incidents. The Cybersecurity Information Handling Guidelines also note that such factors should be weighed against the potential privacy impacts of the continued processing and subsequent use of the PII and the unique nexus of the information to the associated cybersecurity threat or incident.

The ECS PIA uses two sets of terms—"analytically relevant" or "directly relevant" (also "directly related")—to describe the standards for handling information that could be considered PII. Although these terms are sometimes used interchangeably, information that is "directly relevant" to a cybersecurity threat would be an indicator that could be used to actually detect or block the cybersecurity threat. Information that is "analytically relevant" could be information that could be used to detect or block a cybersecurity threat, but it could also be information that is important to understand the nature of the threat. US-CERT may retain either type of information under its Cybersecurity Information Handling Guidelines. If PII must be retained by US-CERT to understand a cybersecurity issue, its retention must be approved by the appropriate DHS oversight offices (the CS&C Compliance and Oversight Officer, NPPD Office of Privacy, the Office of General Counsel, etc.) and labeled with appropriate warnings and markings that PII is included.

[16] Per a request from NPPD, the DHS Privacy Office reviewed five sample signatures provided by NPPD as part of the preparation of the August 2014 follow-up report to the 2012 EINSTEIN PCR. The DHS Privacy Office also reviewed two more recent signatures provided specifically for this PCR. For more information on the August 2014 follow-up report, *see* Letter from Karen L. Neuman to Brendan Goode and Emily Andrew, "Privacy Compliance Review Follow-Up for the EINSTEIN Program," August 26, 2014. Available at: http://www.dhs.gov/sites/default/files/publications/einstein%20pcr%20ltr%20august%202014.pdf.

An example of information that could be considered PII that is directly relevant to a cybersecurity threat is a legitimate e-mail address that may be spoofed from a legitimate website that has been compromised. A bad actor may use the compromised e-mail address to launch a spear phishing[17] campaign. In a spear phishing campaign, the e-mail address is the actual threat vector, so there are no ways to prevent this type of attack without developing a signature to detect e-mails or attachments from that specific e-mail address.

When information that could be considered PII is included in an indicator, because it is information that is directly related to a cybersecurity threat, it is shared with CSPs under ECS as part of the known or suspected cybersecurity threat. Consequently, the information is not marked as information that could be considered PII because it is part of the known or suspected cybersecurity threat and no longer referenced as PII.[18]

Finding and Recommendation:

The DHS Privacy Office finds NPPD to be in compliance with the requirements outlined in the ECS PIA and has no recommendations at this time.

2. Conducting Initial and Periodic Reviews for Data Quality

ECS PIA Requirements:

All indicators are vetted through trusted and validated sources, using unclassified references whenever possible. DHS will conduct periodic reviews on cybersecurity indicators to ensure all standards and responsibilities are met and that the indicator is still operationally relevant.

Review:

The DHS Privacy Office reviewed standard operating procedures related to indicator development, verification, and vetting; oversight analysis of sample signatures; and a written response from NPPD regarding the indicator lifecycle and vetting process. The DHS Privacy Office also conducted follow-up engagement with NPPD.

Results of Review:

DHS performs both initial vetting and periodic reviews that promote data quality in the cybersecurity indicators shared through the ECS Program.

DHS provides data quality criteria to partners that share indicators with DHS. These criteria are used to determine whether an indicator should be included in ECS. All indicators that DHS receives and shares are reviewed by DHS to ensure data quality. As part of this review, the

[17] Spear phishing attacks use e-mail or malicious websites to solicit personal information by posing as a trustworthy organization or individual known to the recipient.
[18] *See* Footnote 15.

US-CERT analyst follows the US-CERT Information Handling Guidelines and standard operating procedures regarding indicators that may contain PII.

In addition to the initial vetting of indicators, US-CERT analysts examine indicators regularly. DHS also requests that partners notify DHS of indicators that the partners believe are no longer a cybersecurity threat, and DHS detasks[19] those indicators for use within ECS. (For more information on the disposition of indicators, see Section F.2.) Finally, DHS oversight officials may recommend that indicators that may contain PII be monitored and subsequently reviewed for activity.

Finding and Recommendation:

The DHS Privacy Office finds NPPD to be in compliance with the requirements outlined in the ECS PIA and has no recommendations at this time.

3. Using Publicly Available Information

ECS PIA Requirements:

DHS does not use commercial data sources under ECS for the purpose of identifying individuals. However, to research cybersecurity threats and indicators, DHS analysts do use information from a range of sources, including commercial sources and publicly available data, for the analysis of cybersecurity threats (i.e., anything that could be found through open source Internet searches, newspaper articles). DHS analysts may correlate public information with specific indicators and threats and identify commonalities and patterns among multiple threats.

Review:

The DHS Privacy Office reviewed the US-CERT Cybersecurity Information Handling Guidelines and a written response from NPPD about US-CERT's use of publicly available information. The DHS Privacy Office also conducted follow-up engagement based on NPPD's written response.

Results of Review:

US-CERT's use of publicly available or "open-source" information is a human-driven process that promotes data quality and adheres to policies and procedures related to protecting PII. US-CERT uses information derived from classified and unclassified reports to research indicators. US-CERT does not request or otherwise seek information associated with specific

[19] "Detask" is the term used when an indicator is removed from operational use in DHS's cybersecurity programs.

persons. Any PII that is determined not to be necessary to understand the cyber threat, analysis, or product will be minimized.[20]

When using publicly available information, US-CERT attempts to verify indicator information against known sources. Any identification of commonalities or patterns is based on a collaborative effort within US-CERT. In performing this analysis, US-CERT analysts must adhere to the US-CERT Cybersecurity Information Handling Guidelines and standard operating procedures concerning PII.

Finding and Recommendation:

The DHS Privacy Office finds NPPD to be in compliance with the requirements outlined in the ECS PIA and has no recommendations at this time.

4. Testing

ECS PIA Requirements:

The indicators are tested for false positive and false negative results in a test environment before they are provided to the CSPs. Additional testing is then performed in the production environment to validate expected results.

Review:

The DHS Privacy Office reviewed a written response from NPPD and conducted follow-up engagement. The DHS Privacy Office also reviewed standard operating procedures related to signature development.

Results of Review:

Although the PIA notes that indicators will be tested for false positive and false negative results, testing is actually part of the signature development process. DHS has robust standard operating procedures in place to perform testing on the signatures that it develops for use in EINSTEIN, but DHS does not test indicators that it shares through ECS. ECS is a voluntary program under which private sector companies provide services to critical infrastructure clients. The CSPs develop their own signatures and are not required to use any indicators provided by DHS. If a CSP chooses to use an indicator to develop a signature, then it would follow its own processes for testing. Consequently, despite what is described in the PIA, DHS does not test the indicators it shares through ECS for false positive and false negative results in a test environment.

[20] PII in US-CERT data that is not necessary to understand the cyber threat is minimized. For example, PII such as a name or an e-mail address that may be *part of* a cyber threat but is not *necessary to understand* the cyber threat (e.g., firstname.lastname@e-mail.com) will be replaced with "PII."

The PIA requires the testing of indicators for false positive and false negative results as a method to ensure the accuracy of the data. Although DHS is not performing the testing described in the PIA as part of the ECS process—and such testing would not necessarily be appropriate for a voluntary program in which CSPs develop and test their own signatures—DHS has other measures to promote data quality. These other data quality protections include initial and periodic review of indicators for data quality, standard operating procedures that seek to minimize the use or collection of unnecessary PII, and a review by oversight officials of signatures that include PII. (For additional information on these data quality measures, see Sections B.1, B.2.) Consequently, the absence of testing as described in the PIA is a transparency issue, but it does not mean that the ECS Program has insufficient data quality protections.

Finding and Recommendation:

The DHS Privacy Office finds that NPPD is not implementing the testing described in the PIA; however, NPPD has other measures to promote data quality. The DHS Privacy Office recommends that NPPD update the ECS PIA to reflect the current state of testing and the existing data quality protections DHS is using in the ECS Program.

C. ECS Services

1. Existing Services – Domain Name System Sinkholing and E-mail Filtering

ECS PIA Requirements:

ECS involves sharing indicators with CSPs and offering two cyber threat services—Domain Name System (DNS) Sinkholing and E-mail Filtering. DNS Sinkholing allows CSPs to redirect traffic from malicious domains to "safe servers" or "sinkhole servers" to prevent further malicious activity. The E-mail Filtering capability allows CSPs to scan, and potentially quarantine, e-mail destined for critical infrastructure companies' networks, in order to detect malicious attachments, Uniform Resource Locators (URLs), and other forms of malware before the e-mail is delivered to company end-users. Services are made available by DHS to the CSPs for implementation with their critical infrastructure clients.

Review:

The DHS Privacy Office reviewed a written response from NPPD and conducted follow-up engagement regarding DHS's access to critical infrastructure company information pursuant to a deployment of DNS Sinkholing or E-mail Filtering services.

Results of Review:

DHS does not collect PII or access the contents of CSPs' communications through DNS Sinkholing or E-mail Filtering services. With respect to the DNS Sinkholing service, the CSPs supply the hardware that supports the Safe Servers. DHS provides virtual images of the Safe

Servers for the CSPs to use. CSPs separately provide DHS with metrics for services received under the ECS Program. For the DNS Sinkholing service, CSPs share metrics on the "hits" on the Safe Servers. The provision of these metrics does not allow DHS to access the Safe Servers. The original software for the Safe Servers came with the capability to collect metrics, but the software was modified to remove that capability as part of privacy-by-design. Consequently, DHS does not have access to the Safe Servers after they are provided to the CSPs. (For more information on CSPs' sharing metrics with DHS, see Section G.1.)

Under the E-mail Filtering service, the CSP actually develops the e-mail filtering capability. DHS provides the cybersecurity indicators, as well as security requirements to ensure that the filtering capability appropriately protects government-provided indicators from unauthorized disclosure through the service. DHS does receive cybersecurity metrics from the CSPs. However, DHS cannot and does not access content or metadata associated with any messages through the e-mail filtering capability.

Finding and Recommendation:

The DHS Privacy Office finds NPPD to be in compliance with the requirements outlined in the ECS PIA and has no recommendations at this time.

2. Onboarding New Services

Requirements:

When conducting a PCR, the DHS Privacy Office must review changes to the underlying program to determine if the existing PIA must be updated. ECS has separate policies and procedures that govern the addition of new services or features.

Review:

The DHS Privacy Office reviewed NPPD/CS&C's policy principles and standard operating procedure for approving new ECS services. The DHS Privacy Office also reviewed compliance with standard internal DHS processes for making changes to DHS programs.

Results of Review:

NPPD/CS&C adhered to its policies and procedures, including appropriate review of privacy considerations, when it pursued deployment of a new service. (Any new service will be described in an ECS PIA update prior to the deployment of the new service.) These policies and procedures provide opportunity for the DHS Privacy Office and the NPPD Office of Privacy to assess the privacy impacts of proposed new services. NPPD/CS&C's policy for approving new ECS services requires that new services adhere to the Fair Information Practice Principles to minimize adverse impacts on privacy and civil liberties—including a review of proposed services by the DHS Privacy Office and Office for Civil Rights and Civil Liberties—and that the

new services abide by the privacy and civil liberties guidelines already established for the ECS Program.

Finding and Recommendation:

The DHS Privacy Office finds NPPD to be in compliance with DHS and NPPD/CS&C policies and processes for deploying a new ECS service and has no recommendations regarding these policies or processes.

D. Access and Security Controls

1. Access and Security Controls – DHS

ECS PIA Requirements:

ECS information is stored in the NCPS Mission Operating Environment (MOE). The MOE is a protected system with security accreditation that is accessible only to authorized NPPD/CS&C personnel with a need-to-know. User accounts are reviewed monthly to ensure they remain current, user account activity is logged, and the logs are reviewed daily.

Review:

The DHS Privacy Office reviewed a written response from NPPD/CS&C describing the NCPS MOE, its process for providing access to users, its two-factor authentication process, and its security certification. The written response also addressed user account reviews and user activity logging. The DHS Privacy Office conducted follow-up engagement with NPPD and also reviewed the NCPS Computer System Access request forms and terms of use agreements.

Results of Review:

The DHS Privacy Office finds NPPD/CS&C to be in compliance with the requirements outlined in the ECS PIA. Specifically, NCPS MOE is separate from the DHS enterprise, meets Federal Information Processing Standard (FIPS) 199 standards, and applies National Institute for Standards and Technology (NIST) Publication 800-53 controls. Under the NCPS MOE access request process, users' access rights may only be assigned from a pre-defined set of possible rights associated with the organization, sub-organization, and their role. These access rights must be approved by a designated approval authority who verifies the user's need-to-know. To access the system, users must use two-factor authentication. NCPS MOE received a security re-certification on July 22, 2013. As an additional layer of security, access to ECS data within the NCPS MOE is restricted using other security mechanisms, and users are only provided access on a need-to-know basis.

User activities on the NCPS MOE are logged and reviewed by NPPD's Network Security Deployment Division for security purposes. The NCPS user agreements require users to acknowledge they will be subject to monitoring when using NCPS. Logs for the NCPS MOE are

reviewed regularly. The Network Security Deployment Division also performs user account reviews, and accounts that have not been used in the last 30 days are disabled and must be reinstated according to the Network Security Deployment Division's account management process. When an employee or contractor leaves, they must follow a standard check out procedure, which initiates a process to immediately disable that individual's accounts.

These processes may be performed by NPPD offices other than those referred to in the PIA. For example, the PIA notes that the CS&C ISSO reviews the accounts monthly to ensure they are "maintained current." This review is actually performed by NPPD's Network Security Deployment Division. However, the protections described in the PIA are being implemented by DHS.

Finding and Recommendation:

The DHS Privacy Office finds NPPD to be in compliance with the access control requirements outlined in the ECS PIA. The DHS Privacy Office recommends NPPD update the ECS PIA to reflect the current frequency of log reviews.

2. Access and Security Controls – Commercial Service Providers

ECS PIA Requirements:

DHS will provide participating CSPs with security requirements, including those necessary to protect unclassified and classified cybersecurity indicators from unauthorized disclosure.

Review:

The DHS Privacy Office reviewed a written response from NPPD/CS&C regarding the security requirements provided to CSPs, discussed the process with the NPPD Office of Privacy, conducted follow-up engagement with NPPD, and reviewed the MOA template for sharing information with CSPs.

Results of Review:

DHS provides robust security requirements to CSPs designed to protect classified information. These security requirements also help protect ECS information from unauthorized disclosure. Pursuant to its MOA with DHS, a CSP participating in ECS must adhere to a variety of stringent security controls. DHS shares indicators with CSPs through secure channels. CSPs must maintain a secure environment in which they can use ECS information. The requirements for these environments are derived from law and Executive Branch policies, and are not unique to the ECS Program. NPPD's Network Security Deployment Division performs a security assessment and testing to ensure the security requirements are met. Changes to a CSP's system that may have an impact on the system's security posture require coordination with DHS to determine whether additional assessment or testing is needed. CSPs must also have a Computer

Incident Response Plan, which includes activities the CSP must perform such as auditing, monitoring, and responses that would occur should an unauthorized disclosure of information occur.

Finding and Recommendation:

The DHS Privacy Office finds NPPD to be in compliance with the requirements outlined in the ECS PIA and has no recommendations at this time.

3. Unauthorized Disclosures and Incident Response

ECS PIA Requirements:

The security requirements DHS provides to CSPs are designed to protect indicators from unauthorized disclosure. The ECS PIA does not discuss specific requirements for incident response in the event of an unauthorized disclosure. However, DHS has policies and standard operating procedures for incident response, in the event that an unauthorized disclosure were to occur at DHS.

Review:

The DHS Privacy Office reviewed a written response from NPPD, along with the MOA with the CSPs and the NCPS standard operating procedures for incident handling and reporting.

Results of Review:

NPPD received no reports of unauthorized disclosures of indicators through the ECS Program. In the event of an unauthorized disclosure, NPPD would follow DHS and NCPS-specific standard operating procedures for incident handling.

Although the MOA requires CSPs to adhere to security requirements, it does not expressly require CSPs to notify DHS in the event of an unauthorized disclosure of cybersecurity indicators.

However, DHS shares both classified and unclassified indicators with CSPs through secure channels. CSPs receive, store, and use indicators in secure, classified facilities. The use of these secure, classified channels and facilities provides an additional layer of security to prevent the unauthorized disclosure of cybersecurity indicators and triggers some reporting requirements in the event of an unauthorized disclosure. Individuals accessing classified information are required by Executive Branch policies to report any unauthorized disclosures of classified information or unauthorized access to classified facilities or networks.

These requirements are conditions of CSPs' accessing classified information or facilities. Similarly, CSPs are required by the MOA to adhere to the security requirements that DHS provides to them. (For more information on these security requirements, see Section D.2.) Consequently, some notification requirements are built into the ECS Program as a result of its

use of classified channels and facilities for the sharing, storage, and use of both classified and unclassified indicators.

CSPs must also have a Computer Incident Response Plan, and termination of the MOA does not relieve CSPs of their obligation to protect ECS information from unauthorized disclosure.

Finding and Recommendation:

The DHS Privacy Office finds NPPD to be in compliance with the requirements outlined in the ECS PIA and has no recommendations at this time.

E. Notice

ECS PIA Requirements:

All authorized users of the participating critical infrastructure companies' networks will be under written notice, either through an electronic banner or otherwise, that information and data on the network may be monitored or disclosed to third parties or that the network users' communications on the network are not private.

Review:

The DHS Privacy Office reviewed a written response from NPPD and the MOA template for sharing information with CSPs.

Results of Review:

The MOA requires that CSPs, prior to providing ECS services to any protected entity, "obtain a representation from such protected entity that, during the duration of such protected entity's participation in ECS, all authorized users of the protected entity's network will be under written notice, through an electronic login banner or otherwise, that information and data on the network may be monitored or disclosed to third parties, and/or that the network users' communications on the network are not private." The CSPs maintain private contractual agreements with their clients, and DHS is not party to those agreements. In keeping with the voluntary nature of CSPs' participation in the program, DHS does not monitor the CSPs' client-side implementation of ECS to ensure compliance with the terms and conditions of the MOA.

Finding and Recommendation:

The DHS Privacy Office found NPPD to be in compliance with the requirements outlined in the ECS PIA and has no recommendations at this time.

F. Data Retention and Disposition

1. Retention – DHS

ECS PIA Requirements:

When the ECS PIA was issued, DHS was working to determine the appropriate retention period for cybersecurity indicators and related information, including information that could be considered PII.

Review:

The DHS Privacy Office reviewed the NCPS Request for Records Disposition Authority that was submitted to the National Archives and Records Administration (NARA) and a written response from NPPD regarding its progress on establishing an appropriate retention period.

Results of Review:

NPPD has improved the privacy protections described in the PIA by pursuing a records retention schedule for cyber threat information. The NCPS retention schedule covers all cyber threat information and is not broken down by program. Generally, NPPD will destroy or delete cyber threat information when it is three years old or when it is no longer needed for agency business, whichever is later. Information that is inadvertently collected or determined not to be related to known or suspected cyber threats or vulnerabilities will be destroyed or deleted immediately or when it is no longer needed for agency business (e.g., after the completion of analysis). Other exceptions include analysis, reports, and forensic files.

Finding and Recommendation:

The DHS Privacy Office found NPPD to be in compliance with the requirements outlined in the ECS PIA. Now that NPPD has proposed a retention schedule, the DHS Privacy Office recommends that the high-level retention policies for data collected and maintained in NCPS be included in an ECS PIA update.

2. Disposition – DHS

ECS PIA Requirements:

Only information determined to be directly relevant and necessary to accomplish the purpose of the ECS Program will be retained. Otherwise, the data will be deleted. NPPD/CS&C will conduct periodic reviews on cybersecurity indicators to ensure that the indicators are still operationally relevant.

Review:

The DHS Privacy Office reviewed a written response from NPPD describing the cybersecurity indicator lifecycle. The Privacy Office also reviewed documentation on the

cybersecurity indicator vetting process—to include the "detasking"[21] of indicators—and reports on the modification, addition, and detasking of indicators.

Results of Review:

DHS has adopted procedures to ensure that cybersecurity indicators are retained only if they are current cyber threats and are modified or detasked if the cyber threat changes. US-CERT analysts review indicators when they are received to ensure they are still credible cyber threats and follow US-CERT policies and procedures for indicators that may contain PII. US-CERT also performs regular reviews of DHS-developed indicators to determine whether indicators may need to be detasked.

DHS receives cybersecurity indicators from other partners. These partners are asked to notify DHS when they believe an indicator they have provided is no longer a cybersecurity threat. Indicators that are no longer relevant to a cyber threat are also detasked in a timely fashion. NPPD provided reports demonstrating that indicators are regularly detasked.

Finding and Recommendation:

The DHS Privacy Office found NPPD to be in compliance with the requirements outlined in the ECS PIA and has no recommendations at this time.

3. Retention and Disposition – Commercial Service Providers

ECS PIA Requirements:

CSPs are required to return or dispose of indicators in accordance with the ECS MOA, if they choose to terminate their MOA.

Review:

The DHS Privacy Office reviewed a written response from NPPD, the MOA template for sharing information with CSPs, and reports on the modification, addition, and detasking of cybersecurity indicators.

Results of Review:

In the event that a CSP chooses to end its participation in the ECS Program, the MOA requires the CSP to return, or at DHS's option, destroy all information it received as a result of the MOA. The CSP does not have to destroy the actual MOA, its attachments, or any written approvals given under the MOA. Furthermore, the CSP is not obligated to return or destroy any information that was (1) already known to the it prior to DHS's sharing information with the CSP or (2) identified or otherwise obtained by the CSP independently of its access to information from DHS through the ECS Program.

[21] *See* Footnote 19.

No information is provided to a CSP until the provider is approved to be "operational" (i.e., able to begin using the information it receives under ECS). As of the review period of the PCR, no CSP has terminated its MOA after becoming operational and having received information under the ECS Program.

CSPs are not subject to a retention or disposition requirement for the information they receive under the ECS Program, as long as they continue to participate in the program. Because ECS is a voluntary program and CSPs are therefore free to choose whether and when to use an indicator, the MOA with CSPs does not require them to delete an indicator. However, US-CERT does request that the CSPs delete indicators that have been detasked. DHS regularly provides CSPs with a spreadsheet that includes active, modified, added, and deleted indicators. Deleted indicators are detasked by DHS and are not included in future spreadsheets sent to CSPs.

Finding and Recommendation:

The DHS Privacy Office found NPPD to be in compliance with the requirements outlined in the ECS PIA and has no recommendations at this time.

G. Information Sharing

1. Incoming – Commercial Service Provider Feedback to DHS

ECS PIA Requirements:

CSPs may, with the permission of the participating critical infrastructure client, provide limited, anonymized, and aggregated cybersecurity metrics to DHS. This information is limited to the timestamp of the occurrence, the indicator involved, and the identification of the critical infrastructure in which the effected entity is a member. Information such as PII or the client's company name will not be shared with DHS.

Review:

The DHS Privacy Office reviewed standard operating procedures and templates related to metrics, monthly ECS metrics reports, documentation related to ECS services, the MOA template for sharing information with CSPs, and a written response and follow-up information from NPPD regarding its collection of metrics from the CSPs.

Results of Review:

NPPD has developed a variety of controls to ensure that DHS does not receive PII from CSPs participating in the ECS Program.

First, the DHS MOA with CSPs limits the information a CSP may provide to DHS. Consistent with its commercial agreements, a CSP may provide general feedback about its participation in ECS, such as the number of participating critical infrastructure entities, the critical infrastructure sectors that are represented, and identities of the critical infrastructure

entities to which the CSP is providing ECS information; the specific ECS Program services provided to each entity; and the total number of items (e.g., e-mails, DNS queries) scanned against and matched to ECS cybersecurity indicators. Furthermore, CSPs may also provide aggregated cybersecurity metrics grouped by critical infrastructure sector. These aggregated metrics are defined in the MOA and include metrics such as: the number of hits (and source IP addresses) per indicator in a given time period; the number of hits (and source IP addresses) per indicator per customer (name redacted, unless otherwise agreed by customers) per given time period; whether a link or attachment was included in the e-mail and if an attachment was included, the attachment type; and metrics specific to DNS redirection.

Second, DHS asks that CSPs send the metrics (referenced above) to DHS in a standardized spreadsheet format. This standardized format does not include any fields that request PII. CSPs submit the spreadsheet to DHS on a weekly basis. NPPD reported that it has received no metrics from CSPs that include PII. DHS uses these aggregated metrics to develop monthly reports on the performance of the ECS Program. The DHS Privacy Office reviewed 12 of these monthly reports from September 2013 to August 2014, none of which included PII.

Third, DHS considered technical controls to limit the provision of PII to DHS as it deployed ECS Program services. For example, the original software for the Safe Servers DHS provides to CSPs under the DNS Sinkholing service comes with the capability to collect metrics, but the software is modified to remove that capability. Consequently, DHS does not receive information from the Safe Servers after they are provided to the CSPs, and CSPs sending metrics to DHS must do so through the standardized process.

Finding and Recommendation:

The DHS Privacy Office found NPPD to be in compliance with the requirements outlined in the ECS PIA and has no recommendations at this time.

2. Outgoing – DHS's Sharing of Cybersecurity Metrics and Indicators Developed as a Result of the Subsequent Analysis of Cybersecurity Metrics

ECS PIA Requirements:

DHS will share cybersecurity metrics received from CSPs with U.S. Government entities with cybersecurity responsibilities for the purpose of evaluating the performance of the ECS Program. DHS will share this information consistent with its existing policies and procedures.

Review:

The DHS Privacy Office reviewed a written response from NPPD; standard operating procedures for sharing information with law enforcement, intelligence, and international partners; the MOA template for sharing information with CSPs; and the MOA template for

sharing information with Federal NCPS participants. The DHS Privacy Office also conducted follow-up engagement with NPPD based on NPPD's written response.

Results of Review:

Information sharing agreements and standard operating procedures govern DHS's sharing of cybersecurity information with other entities. DHS has information sharing agreements with federal agencies participating in EINSTEIN. Additionally, US-CERT may share information with law enforcement and intelligence partners through liaisons detailed to US-CERT. When sharing with law enforcement and intelligence partners, standard operating procedures require US-CERT to evaluate the relevance of the information to the mission or primary jurisdiction of the partner, as well as other applicable authorities of the partner. US-CERT also has standard operating procedures for sharing with international partners as appropriate.

The MOA between DHS and a CSP limits further dissemination of cybersecurity metrics to federal partners with cybersecurity responsibilities. For example, if a federal partner with cybersecurity responsibilities provides indicators to DHS for inclusion in ECS, then that partner will also receive metrics related to the indicators. These metrics are intended to assist in the evaluation of the performance of the ECS Program.

The MOA contains a provision noting that DHS is not prohibited from deriving cybersecurity indicators, including IP addresses, from the metrics provided by CSPs. The MOA further notes that DHS may use or disseminate any indicators it derives from metrics provided by the CSPs, as long as the derived indicators do not identify the source of such information and are not otherwise attributable to a CSP or any protected entity.

DHS has not exercised this option to date. Instead, the metrics may prompt DHS to look at an indicator in greater depth, and this subsequent analysis may cause DHS to develop additional indicators. Any indicators that DHS may develop through this subsequent analysis would be developed according to US-CERT processes for all cybersecurity indicators. Similarly, those indicators will be shared according to agreements (e.g., participation in EINSTEIN) or standard operating procedures. Any indicators developed through this subsequent analysis—or derived from metrics, should DHS choose to ever exercise that option under the MOA—would have the same privacy protections as those included in all indicator development and would be shared according to DHS's information sharing agreements and standard operating procedures.

Finding and Recommendation:

The DHS Privacy Office found NPPD to be in compliance with the requirements outlined in the ECS PIA. The DHS Privacy Office recommends that NPPD describe in a future ECS PIA update how its subsequent analysis of cybersecurity metrics may lead to the development of new indicators.

H. Training

ECS PIA Requirements:

All DHS employees and contractors are required to complete annual Privacy Awareness Training. CS&C analysts supporting the ECS Program are trained on both DHS and CS&C specific privacy protection procedures. Only trained users have access to the cybersecurity indicators.

Review:

The DHS Privacy Office reviewed NPPD's US-CERT cybersecurity-specific privacy training materials and training schedule; the US-CERT Cybersecurity Information Handling Guidelines, which outline US-CERT's privacy procedures and are the basis for the cybersecurity-specific privacy training; the DHS annual Privacy Awareness Training available through DHScovery; NCPS access request form and use agreements; and metrics on various privacy training programs, including those at NPPD, that are collected semi-annually by the DHS Privacy Office. The DHS Privacy Office also reviewed a written response from NPPD and the DHS Privacy Office lead for the DHS privacy training program.

Results of Review:

DHS has processes in place to ensure all DHS employees receive basic privacy awareness training, and NPPD began implementing the cybersecurity-specific privacy training in June 2014.

All DHS employees and contractors are required to complete annually the computer-assisted privacy awareness training course, "Privacy at DHS: Protecting Personal Information." This standardized training, developed by the DHS Privacy Office, is provided to DHS staff through one of seven different learning platforms. NPPD uses the DHScovery learning platform to complete the annual Privacy Awareness Training. DHScovery sets deadlines for the privacy training, which repeat annually. DHScovery notifies supervisors if employees have not completed training by the required deadline.

Additionally, NPPD developed cybersecurity-specific training based on the US-CERT Information Handling Guidelines, which outline US-CERT's privacy procedures. Although this training was developed after the publication of the PIA in January 2013, NPPD has made a robust attempt to develop and implement in-depth, context-specific training for its analysts. After the US-CERT Cybersecurity Information Handling Guidelines were approved in August 2013, NPPD developed training material based on the guidelines and completed its first iteration of cybersecurity-specific privacy training in June 2014. This training is managed by the National Cybersecurity and Communications Integration Center (NCCIC) Oversight and Compliance Officer and is conducted quarterly or as necessary to accommodate new analysts at NPPD. NPPD uses occupational codes and job descriptions to identify analysts who must receive the

cybersecurity-specific privacy training. After the first iteration, additional sessions were conducted in July, August, and September 2014, and NPPD has trained 86 analysts as of September 2014.

The cybersecurity-specific training provides an overview of basic privacy concepts; identifies key triggers of privacy requirements in US-CERT's work; provides an in-depth review of requirements related to US-CERT's collection, processing, safeguarding, retention, and dissemination of information; outlines various accountability mechanisms for US-CERT's handling of PII; and provides a list of resources (e.g., points of contact, specific standard operating procedures) for analysts to use later.

Finding and Recommendation:

The DHS Privacy Office found NPPD to be in compliance with the requirements outlined in the ECS PIA and has no additional recommendations at this time.

I. Oversight and Accountability

ECS PIA Requirements:

To ensure that the information is used in accordance with the ECS PIA, the CS&C Oversight and Compliance Officer and NPPD Senior Privacy Analyst conduct quarterly internal reviews to evaluate and assess compliance with the information handling procedures as outlined in the standard operating procedures.

Review:

The DHS Privacy Office reviewed reports of Quarterly Privacy Reviews from the fourth quarter of fiscal year 2012 to the third quarter of fiscal year 2014.

Results of Review:

The Quarterly Privacy Reviews provide an opportunity for DHS oversight officials to conduct a timely and in-depth analysis of CS&C/US-CERT's information handling procedures. The reviews cover an impressive array of topics, including but not limited to: any privacy incidents; standard operating procedures and checklists; reviews of signatures and signature templates; information sharing activities; and retention. As a result of these reviews, NPPD is able to identify privacy risks and mitigations as the program evolves and matures.

Finding and Recommendation:

The DHS Privacy Office found NPPD to be in compliance with the requirements outlined in the ECS PIA and has no recommendations at this time.

IV. Conclusion

The DHS Privacy Office continues to work collaboratively with NPPD to ensure implementation of ECS in a privacy-sensitive manner. NPPD worked diligently with the DHS Privacy Office to create privacy protective enhancements to ECS and its related processes during the development of the program. NPPD also worked closely with the DHS Privacy Office during the 2011 PCR of EINSTEIN, and we appreciate NPPD's diligence in having implemented those recommendations, as evidenced by the 2013 review of NPPD's implementation of the 2011 recommendations. The sensitivities surrounding cybersecurity programs, and the requirement for cooperation between the public and private sectors in particular, require robust privacy oversight. NPPD has demonstrated exemplary attention to implementing strong privacy protections in ECS and its related processes, and the DHS Privacy Office recommends NPPD take the following steps to further strengthen its privacy protections in ECS and its related processes:

- *Recommendation 1:* NPPD should update the ECS PIA to better reflect the current state of indicator testing and the existing data quality protections DHS is using in the ECS Program.
- *Recommendation 2:* NPPD should update the ECS PIA to reflect the current frequency of log reviews.
- *Recommendation 3:* NPPD should provide updated information about indicator retention in a future ECS PIA update.
- *Recommendation 4:* NPPD should describe in a future ECS PIA update how its subsequent analysis of cybersecurity metrics may lead to the development of new indicators.

We discussed these recommendations with NPPD, the NPPD Office of Privacy, and the DHS Privacy Office Compliance Team, who are taking steps to implement them. The DHS Privacy Office will conduct a follow-up PCR twelve (12) months from the publication of this PCR to assess the status of the recommendations.

V. Privacy Compliance Review Approval

Responsible Official

Andy Ozment
Assistant Secretary
Cybersecurity and Communications
National Protection and Programs Directorate

Approval Signature

Original signed copy on file with the DHS Privacy Office.

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security