Privacy Impact Assessment
for the

Enhanced Cybersecurity Services (ECS)

DHS/NPPD/PIA-028

January 16, 2013

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

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Enhanced Cybersecurity Services (ECS) is a voluntary program based on the sharing of indicators of malicious cyber activity between Department of Homeland Security (DHS) and participating Commercial Service Providers. The purpose of the program is to assist the owners and operators of critical infrastructure to enhance the protection of their systems from unauthorized access, exploitation, or data exfiltration through a voluntary information sharing program. ECS consists of the operational processes and security oversight required to share unclassified and classified cyber threat indicators with companies that provide internet, network, and communication services to enable those companies to enhance their services to protect U.S. Critical Infrastructure entities. ECS is intended to support U.S. Critical Infrastructure, however, pending deployment of EINSTEIN intrusion prevention capabilities, ECS may also be used to provide equivalent protection to participating Federal civilian Executive Branch agencies. The National Protection and Programs Directorate (NPPD) is conducting this Privacy Impact Assessment (PIA) because personally identifiable information (PII) may be collected. This PIA consolidates and serves as a replacement to the DHS/NPPD/PIA-021 National Cyber Security Division Joint Cybersecurity Services Pilot PIA, published on January 13, 2012, and the DHS/NPPD/PIA-021(a) National Cyber Security Division Joint Cybersecurity Services Program (JCSP), Defense Industrial Base (DIB) – Enhanced Cybersecurity Services (DECS) PIA Update, published on July 18, 2012.

Overview

ECS is the latest evolution of the government's efforts to enhance the cybersecurity of critical infrastructure and other private sector networks. Under the Joint Cybersecurity Services Pilot (Pilot), DHS, through its Office of Cybersecurity & Communications (CS&C), partnered with the U.S. Department of Defense (DoD) to share cyber threat[1] indicators[2] and other information about known or suspected cyber threats with Commercial Service Providers (CSP).[3] The Pilot began as a DHS/DoD joint proof of concept that extended the existing operation of the

[1] 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.
[2] An indicator can be defined as human-readable cyber data used to identify some form of malicious cyber activity and are data related to IP addresses, domains, email headers, files, and strings. Indicators can be either unclassified or classified. Classification of identified indicators is dictated by its source.
[3] The term Commercial Service Provider (CSP), refers to a public or private company that transports information electronically in the wireline, wireless, Internet, cable, satellite, and managed services businesses. Any managed security service provider meeting the eligibility requirements may become a CSP.

DoD DIB Exploratory Cybersecurity Initiative (DIB Opt-in Pilot),[4] and shifted the operational relationship with the CSPs in the DIB Opt-in Pilot to DHS. The purpose of the Pilot was to enhance the cybersecurity of participating DIB critical infrastructure entities and to protect them from unauthorized access, exfiltration, and exploitation. The Pilot was commissioned for 180 days and during that time met its goal to effectively share cyber threat information with CSPs for the purposes of protecting participating DIB companies.

In May 2012, the U.S. Government established the Pilot as an ongoing voluntary program, originally known as the Joint Cybersecurity Services Program (JCSP), and now as the Enhanced Cybersecurity Services (ECS) program. The first phase of ECS focused on the cyber protection of the DIB companies participating in the DOD's Cyber Security Information Assurance Program. DHS is now expanding the ECS to include cybersecurity services for all U.S. Critical Infrastructure (CI) sectors. See Appendix 1 for a list of Critical Infrastructure Sectors. ECS will extend enhanced cybersecurity protection to all of the U.S. CI sectors through the sharing of indicators of malicious cyber activity with CSPs. ECS enables private sector CSPs to provide enhanced protection to CI companies that choose to participate in the program, protecting them from unauthorized access, exploitation, data loss and manipulation, and exfiltration by threat actors. ECS is intended to augment, not replace, existing security services operated by or available to CI companies and does not involve government monitoring of any private networks or communications. Pending deployment of EINSTEIN[5] intrusion prevention capabilities, ECS cyber protection capabilities will continue to be available to interested Federal civilian Executive Branch agencies. Generally, ECS will use the same cyber protection capabilities for Federal civilian Executive Branch agencies as it will for CI sectors. Any differences in how the Federal civilian Executive Branch agencies will be implemented will be described in this PIA.

CS&C

As part of its mission to promote the protection of cyber infrastructure, CS&C analyzes information that is specific to identifying known or suspected cyber threats from a number of sources in the form of "indicators" (e.g., Internet Protocol (IP) addresses, domains, e-mail headers, files, and strings). These "indicators" can be used to create intrusion detection signatures[6] or other means of detecting and mitigating cyber threats. Sources for the collection

[4] For the PIA that covers the DOD DIB Opt-in Pilot see the DoD DIB Cyber Security/Information Assurance Activities PIA at http://dodcio.defense.gov/Portals/0/Documents/DIB%20CS-IA%20PIA_FINAL_signed_30jun2011_VMSS_GGMR_RC.pdf.

[5] Privacy Impact Assessments for DHS cybersecurity programs, including EINSTEIN, can be found at: http://www.dhs.gov/files/publications/editorial_0514.shtm#4.

[6] 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

of these indicators include: cybersecurity analysis activities conducted by DHS; domestic and international private sector organizations; and international, federal, or state agencies with a vested interest in promoting cybersecurity. Indicators about known or suspected cyber threats may also be collected from information gathered by the EINSTEIN sensors placed on Federal civilian Executive Branch agency network collection points.[7]

A cyber indicator (indicator) can be defined as human-readable cyber data used to identify some form of malicious cyber activity and are data related to:

1) IP addresses;
2) Domains;
3) E-mail headers;
4) Files; and
5) Strings.

Each characteristic of an indicator contains specific features, for instance:

- IP and Domain Indicators can contain Uniform Resource Identifiers[8] (URI), and can typically be found in WHOIS[9] publicly available information;
- E-mail Indicators can contain message attributes such as the sent date, subject, links, attachments, sender's name, and sender's e-mail address;
- File Indicators can contain information on malicious software (malware) that is designed specifically to damage or disrupt a computer system, such as the file's size; and
- String Indicators consist of persistent and unique identifiers specific to malicious activity, such as characters, numbers, or symbols, used to represent a word or phrase.

Indicators may contain any of the above at varying levels of detail regarding a cyber threat and one indicator can have a relationship with another indicator. For example: an e-mail may contain an attachment and that attachment may contain malware. These indicators whether separately or grouped together are referred to and submitted as "indicator reports." Indicator

known computer virus that is designed to delete files from a computer without authorization.

[7] These sensors capture flow records that identify the Internet Protocol (IP) address and domain/hostname information 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.

[8] URI is the generic term for all types of names and addresses that refer to objects on the World Wide Web. A Uniform Resource Locator (URL) is one kind of URI.

[9] WHOIS is a Transmission Control Protocol (TCP)-based transaction-oriented query/response protocol that is widely used to provide information services to Internet users. While originally used to provide "white pages" services and information about registered domain names, current deployments cover a much broader range of information services. The protocol delivers its content in a human-readable format.

reports can be produced with any combination of indicators and can have either a single indicator or multiple types of indicators and multiple entries for each type therein. For example: a certain indicator report may contain one email, one file, and one domain; other indicator reports may contain four files, or two domains, and three IP addresses. Indicators and indicator reports are created and validated by CS&C cybersecurity analysts based on indicators of known or suspected cyber threats that are identified and validated by CS&C, private sector organizations, and other partner government agencies. Indicators relate to known or suspected cyber threats and may contain information that could be considered PII, such as e-mail addresses, domain names, or IP addresses.

CS&C 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 email address or an IP address and domain information. In the context of ECS, these types of information are not used to identify an individual; instead, they are used as a reference point for particular known or suspected cyber threats. For example, if the author of a cyber threat chose to use a fraudulent (spoofed) email address in the "from" field in a phishing email threat,[10] an indicator may be developed in response to that cyber threat that would include the spoofed email address. A similar situation could occur when a threat actor uses a particular IP address or domain as a destination for malicious data exfiltration or as part of a "command and control" function. In both of these examples, ECS is not using the email address or IP address as PII (that is, not as a way to identify a particular individual associated with that email address), or even as general information about any specific person; it is simply an indicator of a potential cyber threat. CS&C is only using this information to better identify a known or suspected cyber threat against computer networks. CS&C may establish indicators with information that could be considered PII, but only if the information has proved to be analytically relevant to understanding the known or suspected cyber threat.

In these situations, when an indicator contains information that could be considered PII, CS&C will follow defined Standard Operating Procedures (SOP) and cybersecurity information handling guidelines. Specifically, CS&C will review data and information received to determine whether the information contains PII incidentally present during the investigation, research, and creation of CS&C reports or other products. This type of information would only be shared after its reviewed and determined to be an indicator of a known or suspected cyber threat. If PII is discovered and is determined not to be directly relevant to the cyber threat being analyzed, the information will be handled in accordance with the appropriate SOP. CS&C follows SOPs in

[10] The Melissa virus (http://www.cert.org/advisories/CA-1999-04.html) propagates in the form of an email message containing malicious code as an attachment.

which the analyst will overwrite, redact, or replace PII data that is not necessary to understand the analysis or product.

Indicator Sharing Under ECS

ECS establishes a construct for CS&C to share unclassified and classified indicators of malicious cyber activity with CSPs on behalf of an ECS participant.[11] CS&C identifies those indicators that are critical for protecting CI and shares that information with participating CSPs through secure communication channels. The CSPs configure the indicators into "signatures," which are machine-readable software code that enable automated detection of the known or suspected cyber threats associated with the indicators.[12]

The relationship between CSPs and DHS will be governed through the ECS Memorandum of Agreement (MOA) and the relationship between CSPs and participating entities will be governed through commercial agreements. CS&C is not a party to those agreements.

When CSPs implement a signature on behalf of an ECS participant and that signature triggers an alert, the CSP notifies the participating entity in accordance with its commercial agreement and any applicable security requirements. The CSP may, with the permission of the participating entity, also provide limited, anonymized, and aggregated, cybersecurity metrics information to CS&C sufficient to understand the performance of the ECS program, including the effectiveness of an indicator in preventing an associated known or suspected cyber threat. The information provided is limited to the timestamp of the occurrence, the indicator involved, and the identification of the CI sector in which the affected entity is a member. Information such as the company name or other identifiable information associated with a specific incident will not be shared. When a CSP implements a signature on behalf of a Federal civilian Executive Branch agency participating in ECS and that signature triggers an alert, the CSP shares the same summary information with CS&C as it would for a CI company.

CS&C will share information it receives regarding cyber threats under ECS consistent with its existing policies and procedures, including to other U.S. government entities with cybersecurity responsibilities.

CS&C maintains ECS-related data and information in the National Cybersecurity Protection System (NCPS) Mission Operating Environment (MOE), a CS&C protected system

[11] ECS participants include CI companies and any potential participating Federal civilian Executive Branch departments and agencies that choose to participate in the program through a CSP to protect them from unauthorized access, exploitation, data loss and manipulation, and exfiltration by threat actors.
[12] Additional information about indicators and signatures is addressed in the National Cybersecurity Protection System (NCPS) PIA published on July 30, 2012, and can be found at: http://www.dhs.gov/sites/default/files/publications/privacy/privacy-pia-nppd-ncps.pdf.

on a protected network accessible to only authorized CS&C personnel with a need to know. CSPs maintain government provided indicators of malicious cyber activity in accordance with requirements defined in the ECS MOA. If CSPs choose to terminate the ECS MOA, they must return, or dispose of indicators in accordance with the ECS MOA. In addition to the information described above, CSPs may also voluntarily provide CS&C with lessons learned or other general feedback about ECS technical or operational issues and solutions.

Initial Implementation of ECS

ECS will initially involve the implementation of two cyber threat countermeasures: 1) DNS Sinkholing and 2) Email Filtering.[13] The DNS Sinkhole capability allows CSPs to prevent malware installed on CI company networks from communicating with known or suspected malicious Internet domains by redirecting the network connection away from the malicious domain to "safe servers" or "sinkhole servers", thus preventing further malicious activity by the installed malware. The CSP has access to the sinkhole information. However, it should be noted that the information related to the attempted connection that can be gathered by the service provider is limited to information related to the DNS request rather than the contents of the intended malicious communication. The Email Filtering capability allows the CSPs to scan, and potentially quarantine, email destined for CI companies networks for malicious attachments, Uniform Resource Locators (URL), and other forms of malware, before being delivered to CI company end-users.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

ECS is being conducted pursuant to authority derived from the Homeland Security Act, including 6 U.S.C. §§ 121(d), 133(g), 143; Homeland Security Presidential Directive 7 §§ 12, 16, *Critical Infrastructure Identification, Prioritization, and Protection*; and Homeland Security Presidential Directive 23/National Security Presidential Directive 54, *Comprehensive National Cybersecurity Initiative* §§ 23, 24.

[13] Based on the effectiveness of the program and the evolution of the threat, DHS may add additional countermeasures to ECS, but the potential collection and use of PII will remain unchanged.

The relationship between CSPs and DHS will be governed through the ECS MOA and the relationship between CSPs and participating entities will be governed through commercial agreements. CS&C is not a party to those agreements.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

With regard to indicators or other information related to a known or suspected cyber threat, CS&C does not maintain that information in a "system of record." As defined by the Privacy Act, a "system of records" is a group of any records under the control of any agency from which information is maintained and retrieved by a personal identifier. Only when there is actual retrieval of a record by a personal identifier does the Privacy Act require a SORN. CS&C does not retrieve this information by personal identifier, thus a SORN is not required for ECS.

CS&C collects general contact information from representatives of the CSPs and federal agencies participating in the ECS. This collection of personal information is covered by the DHS systems of records titled, DHS/All- 002 Department of Homeland Security (DHS) Mailing and Other Lists System, November 25, 2008, 73 FR 71659.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

ECS information will be stored in the NCPS MOE, which is a protected system designated to perform threat analysis and other functions. Within ECS, CS&C will share indicators of known or suspected cyber threats from the MOE with CSPs. The MOE received re-certification and accreditation on July 28, 2010, and is covered by the system security plan. The re-certification is valid for three years.

The ECS program is purely voluntary. However, as a condition of participation, DHS will provide CSPs with security-related requirements to protect ECS program equities, sources and methods. Within ECS, the term Security Requirements refers to those requirements provided to CSPs necessary to protect unclassified and classified indicators of malicious cyber activity from unauthorized disclosure.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

CS&C is currently working with the NPPD Records Manager to develop a disposition schedule that will cover all NCPS information, to include ECS.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Information is not being collected or solicited directly from the public therefore the Paperwork Reduction Act is not applicable in this situation. While information is being collected, it is not done so through the solicitation of the same questions from 10 or more persons and in a manner that is consistent with PRA requirements.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

ECS is voluntary and is based on the sharing of U.S. Government provided indicators of malicious cyber activity with CSPs. CS&C provides indicators to CSPs for the purpose of enhancing the protection of ECS participants. The CSPs, at the request of ECS participants, in turn use such indicators to look for known or suspected cyber threats transiting to and from ECS participant network traffic. As part of the program, the CSPs may share summary information with CS&C about the fact that known or suspected cyber threats were detected. This "fact of" occurrence reporting will not contain information that could be considered PII.

The following information that could be considered PII may be part of E-mail indicators shared through the ECS: attributes such as the sender's name, sender's e-mail address, and information from and associated with email messages, as well as other information that could be contained in the message header, to/from free-flow text fields, or subject line from individuals using federal websites or ECS participants' networks and systems. CS&C will review all information it receives for the ECS and only retain information that could be considered PII if that information is analytically relevant to understanding the cyber threat. In these situations, when an indicator contains information that could be considered PII, CS&C will follow defined Standard Operating Procedures (SOP) and cybersecurity information handling guidelines. Specifically, CS&C will review information received to determine whether that information contains PII incidentally present during the investigation, research, and creation of CS&C reports or other products. This type of information would only be shared after review and determined to be an indicator of a known or suspected cyber threat. If PII is discovered and is determined not to be directly relevant to the cyber threat being analyzed, the information will be handled in

accordance with the appropriate SOPs, which includes the overwrite, redaction, or replacement of PII that is not necessary to understand the analysis or product.

As part of ECS, CS&C collects general contact information from representatives of the CSPs and federal agencies participating in the ECS, to include employee name, business address, business telephone number, and business email address. This contact information is used by CS&C as part of daily operations for the program.

2.2 What are the sources of the information and how is the information collected for the project?

Indicators and other cyber threat related information are received by CS&C from a number of sources[14] including the following: cybersecurity analysis activities conducted by DHS; domestic and international private sector organizations; and international, federal, or state agencies with a vested interest in promoting cybersecurity. Indicators about known or suspected cyber threats may also be collected from information gathered by the EINSTEIN sensors placed on Federal civilian Executive Branch agency network collection.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

CS&C analysts do not use commercial sources for the purpose of identifying individuals. CS&C 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, etc.). As an example, indicator information obtained from WHOIS data provides analysts with the ability to enhance existing analysis records by correlating information contained in a WHOIS record with specific indicators and threats, and identify commonalities and patterns among multiple threats.

2.4 Discuss how accuracy of the data is ensured.

All indicators are vetted through trusted and validated sources, using unclassified references for indicators whenever possible. The indicators are tested for false positive and false

[14] As noted in the NCPS PIA, the exchange of information on cybersecurity occurs between DHS, department and agencies, intelligence agencies, state, local, tribal governments, private organizations, foreign Computer Security Incident Response Teams (CSIRT), and the public. This sharing is done in accordance with MOAs or other types of information sharing agreements, as applicable.

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.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that information that could be considered PII is included in an indicator when that information does not add any value to the prevention of a known or suspected cyber threat.

Mitigation: CS&C only collects information that is necessary to accomplish its mission; cyber threat (i.e., indicator) information, as described in the Overview, may include information that could be considered PII. CS&C analysts attempt to confirm the integrity of the data received. Only information determined to be directly relevant and necessary to accomplish the specific purposes of the program will be retained, otherwise, the data is deleted.

CS&C will conduct periodic reviews on cyber indicators to ensure all standards and responsibilities are met and that the indicator is still operationally relevant.

Privacy Risk: There is a risk that the indicator does not meet the CS&C standards of quality or applicability and is shared to the detriment of individuals who communicate electronically with the users' organizations or agency.

Mitigation: CS&C has established a process by which only trained and authorized users have access to the indicators. Users must abide by specific rules of behaviors and responsibilities with regard to access and to the quality of the data in NCPS systems. CS&C analysts conduct analysis on all cyber threats received. If a threat submitted contains information that could be considered PII, the analyst must determine if that information is directly related or analytically relevant to the cyber threat. Any information that is not directly relevant to the cyber threat is deleted in accordance with CS&C information handling guidelines and SOPs.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

CS&C provides cybersecurity indicators to CSPs for the purpose of enhancing the network protection of ECS participants. The CSPs, at the request of ECS participants, in turn use such indicators to look for known or suspected cyber threats transiting to and from ECS participant network traffic. As part of the program, the CSPs may share summary information

with CS&C about the fact that known or suspected cyber threats were detected. This "fact of" occurrence reporting will not contain information that could be considered PII.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No; ECS does not use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly.

3.3 Are there other components with assigned roles and responsibilities within the system?

There are no other components with assigned roles and responsibilities within the ECS.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk that PII inadvertently obtained will not be properly protected and will be disseminated to other entities with a potential to lead to unauthorized use of the PII.

Mitigation: CS&C will not receive PII from the CSPs. Aspects of the ECS are governed by information sharing agreements with CSPs, internal CS&C SOPs, existing NPPD PIAs for the NCPS, EINSTEIN, and this PIA, which cover the use of government furnished information, including indicators, collected or maintained. ECS participants maintain contractual relationships established between those entities and their respective CSPs. CS&C is not a party to these agreements.

CS&C analysts supporting the ECS are trained on both DHS and CS&C specific privacy protection procedures. Analysts, administrators, and information assurance personnel receive training upon hire, and are required to take refresher training each year on Security Education and Awareness Training (SEAT). In addition, CS&C maintains SOPs and information handling guidelines, which describe necessary procedures, define the terms, and outline roles and responsibilities for handling PII.

In addition, access to NCPS systems is restricted to authorized government and contractor staff with demonstrated need for access, and such access must be approved by the supervisor as well as the CS&C Information System Security Manager (ISSM)/Security

Manager. Users must sign Rules of Behavior, which identify the need to protect PII prior to gaining access. NCPS users' actions are logged and they are aware of that condition. Failure to abide by the Rules of Behavior may result in disciplinary measures and potential termination of employment.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

This PIA serves as general notice of ECS. All DHS cybersecurity PIAs as well as other information on federal government cybersecurity programs and protections are available on the DHS Privacy Office cybersecurity webpage at: www.dhs.gov/privacy.

All authorized users of the participating CI company'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.

With respect to any Federal civilian Executive Branch agencies participating in ECS, the participating Federal civilian Executive Branch agency's website privacy policy provides notice that the agency uses computer security programs to monitor network traffic. Government users inside the agency network receive notice by their agency's use of logon banners and user agreements notifying agency personnel that their communications or data transiting are stored on the agency network and that network traffic is subject to monitoring and disclosure for network security and other lawful government purposes.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

All authorized users of the CI participant'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. Users have the opportunity to read these notices and can then decide if they wish to use the system or not, and decide what information they want to transmit.

With respect to any Federal civilian Executive Branch agencies participating in ECS, all authorized users logging into their participating agency's IT systems are presented with an electronic notice or banner that notifies them that government computer systems are monitored.

Notice to the public is provided on a participating Federal civilian Executive Branch agency's public facing website privacy policy. The participating Federal civilian Executive Branch agency website privacy policy states that the agency uses computer security programs to monitor network traffic.

Once an individual decides to communicate with a participating agency electronically, the network traffic will be subject to computer security efforts of CS&C, including in this case ECS, in addition to any individual computer security programs the agency might have in place.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a privacy risk that an individual may not be aware of the information collection occurring under ECS.

Mitigation: All authorized users of the CI participant'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. Users have the opportunity to read these notices and can then decide if they wish to use the system or not, and decide what information they want to transmit.

With respect to any federal civilian Executive Branch agencies participating in ECS, the participating federal civilian Executive Branch agency's website privacy policy states that the agency uses computer security programs to monitor network traffic. Government users inside the agency networks receive notice by the agency's use of logon banners and user agreements notifying agency personnel that their communications or data transmissions are stored on their agency's network and that network traffic is subject to monitoring and disclosure for network security and other lawful government purposes. Individuals may also access the existing publicly available DHS Cybersecurity PIAs or visit the DHS Privacy website that also provides resources that explain the DHS cybersecurity mission and programs. See: www.dhs.gov/privacy.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

CS&C is currently working with the NPPD Records Manager to develop disposition schedules that will cover data collected and maintained under the NCPS, to include the ECS. Once completed, the schedule will be sent to NARA for approval.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information that could be considered PII may be retained beyond what is necessary to appropriately analyze or address a cyber threat or investigation.

Mitigation: CS&C is currently working to determine the appropriate length of time for cyber indicators and related information, including information that could be considered PII identified as related to a known or suspected cyber threat to be retained and stored.

CS&C cybersecurity analysts are required to review cyber indicators and related information collected to determine whether information that could be considered PII exists and whether it analytically relevant to a cybersecurity threat. CS&C guidelines and SOPs provide the procedures for this review.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Under ECS, CS&C shares indicators with CSPs for the purpose of enhancing the network protection of ECS participants. The sharing of information between the parties is accomplished through secure communication. Only those individuals that maintain appropriate security clearances and have completed the appropriate training will be granted access to the information.

CS&C also shares cybersecurity metrics information with U.S. Government entities with cybersecurity responsibilities for the purpose of evaluating the performance of the ECS program.

Contact information from representatives of the participating CSPs, and Federal civilian Executive Branch agencies will not be shared outside of normal agency or ECS operations.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Collection of contact information for CSPs described in 6.1 is covered by the DHS systems of records titled, DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, November 25, 2008, 73 FR 71659. CS&C will share this data in a manner that is compatible with the purpose of the aforementioned systems of records notice.

6.3 Does the project place limitations on re-dissemination?

CS&C only shares cybersecurity metrics information with U.S. Government entities with cybersecurity responsibilities for the purpose of evaluating the performance of the ECS program. Metrics will focus on the following areas:

- Performance: related to the performance of indicators and information sharing.
- Participation: related to interest and participation among CSPs and CI to understand the interest and participation in ECS over time.
- Value: related to the value or quality of the information shared from both the Government and Privacy Sector perspectives.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

CS&C only shares cybersecurity metrics information with U.S. Government entities with cybersecurity responsibilities for the purpose of evaluating the performance of the ECS program.

As part of its overall cybersecurity operations mission, CS&C provides cyber-related information to the public, federal departments and agencies, state, local, tribal, and international entities through a variety of products, many of which are available on the US-CERT.gov website. Informational reports disseminated through the US-CERT.gov public website do not contain PII. Each report is numbered and catalogued and references exist in all products (including those associated with indicators shared through the ECS) to tie back to a single incident or series of incidents which precipitated the product itself. In the event that PII must be released, it is released in accordance with the appropriate SOPs and with the authorization and/or written approval of CS&C leadership and in compliance with the Privacy Act. [15]

[15] Approval is not required when information about a specific person is believed to be fictitious, when the information is publicly available, or when the release of such information is being coordinated with the person about whom it is associated.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a privacy risk that CS&C may share indicators with CSPs that contain PII that is not associated with a known or suspected cyber threat.

Mitigation: Unauthorized disclosure is mitigated through various means, including CS&C SOPs and information handling guidelines. CS&C SOPs provide procedures for removing unnecessary PII, securing or encrypting PII, and marking and handling of PII data collected.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

CS&C only maintains contact information for CSPs in a Privacy Act system of records. For individuals seeking access to such records or seeking to amend the accuracy of its content may submit a Freedom of Information Act (FOIA) or a Privacy Act (PA) request to the DHS/NPPD FOIA Officer at 245 Murray Lane SW, Washington, D.C. 20528-0380. Individuals may obtain directions on how to submit a FOIA/PA request at http://www.dhs.gov/xfoia/editorial_0316.shtm.

The release of information not covered by the Contact List System of Records Notice under the Privacy Act may be subject to FOIA Exceptions. Given the nature of some information in the CS&C systems, CS&C may not always be able to give access to information maintained by CS&C.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

CS&C collects general contact information from representatives of the CSPs and Federal civilian Executive Branch agencies participating in the ECS. CSPs and Federal civilian Executive Branch agencies participating in ECS seeking to correct contact information collected by CS&C may contact CS&C directly or submit a written request to DHS/NPPD FOIA Officer at 245 Murray Lane SW, Washington, D.C. 20528-0380, to have their inaccurate or erroneous PII corrected. See additional information in Section 7.1.

There are no separate procedures for individual correction of indicators since the information is generated from exact copies of computer network traffic.

7.3 How does the project notify individuals about the procedures for correcting their information?

As part of normal CS&C operations, CS&C provides notice about procedures for correcting PII to those individuals that submit general contact information as representatives of the ECS program or regarding a suspected or known cyber threat through the applicable SORN, this PIA, and related NPPD PIAs.

An individual can submit a written request to DHS/NPPD FOIA Officer at 245 Murray Lane SW, Washington, D.C. 20528-0380, to have their inaccurate or erroneous PII corrected. See additional information in Section 7.1.

7.4 Privacy Impact Analysis: Related to Redress

There are no redress procedures beyond those described above and afforded under the Privacy Act and FOIA.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

Quarterly internal reviews are carried out by the CS&C Oversight and Compliance Officer, along with the NPPD Senior Privacy Analyst, to evaluate and assess compliance with the information handling procedures as outlined in the CS&C SOPs. Additionally, specific information handling SOPs to ensure awareness, accountability, and compliance of what information should and should not be shared, are circulated annually to the CS&C analysts.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

Access to DHS systems is restricted to individuals with demonstrated need for access, and such access must be approved by the supervisor as well as the CS&C ISSM/Security Manager. Users must sign Rules of Behavior, which identify the need to protect PII prior to gaining access. Access is only available via two factor authentication. All users are trained to protect privacy information. Their actions are logged, and they are aware of that condition.

Failure to abide by the Rules of Behavior may result in disciplinary measures and potential termination of employment.

All DHS employees (and contractors) are required to complete annual Privacy Awareness Training. When each DHS employee completes the training, it is recorded in the employee's file online. NPPD employees and contractors are also required to complete annual Security Education and Awareness Training (SEAT). In addition, CS&C personnel who support or use the NCPS receive annual training on privacy, legal, civil rights and civil liberties, and policy issues specifically related to CS&C operations. This training includes how to address privacy during the development of new signatures, including minimization of PII how to generate a report that minimizes the privacy impact, and how to report when a signature seems to be collecting more network traffic than is directly required to analyze the malicious activity.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Users must obtain a favorable DHS suitability determination[16] prior to acquiring access to all DHS systems. The NCPS provides the technical foundation for CS&C activities, including the ECS. All users supporting ECS have a valid requirement to access the NCPS systems and only the type of access required to meet their professional responsibilities. Access is based upon the role identified on the access form (i.e. analyst, user, general user, system admin., network admin., etc.). The access form must be completed by the government supervisor within the branch that the individual will be supporting. The user's role is defined by the branch manager and validated by the CS&C ISSM/Security Manager. Accounts are reviewed monthly by the CS&C ISSO to ensure that accounts are maintained current. In addition, user account activity is logged, and the logs reviewed each day.

In addition, CS&C maintains SOPs on privacy protection for the purpose of identifying sensitive information, and for the proper handling and minimization of PII, which outlines the necessary procedures and defines the terms for specifically identified roles and responsibilities. These operating procedures are provided to all CS&C operations staff during training and are circulated to CS&C analysts so that they are aware of what information should and should not be shared with its information sharing partners.

[16] The suitability determination is a process that evaluates a federal or contractor employees' personal conduct throughout their careers. Suitability refers to fitness for employment or continued employment referring to identifiable character traits and past conduct that is sufficient to determine whether or not an individual is likely to carry out the duties of the position with efficiency, effectiveness, and in the best interests of the agency.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

The Memoranda of Agreements (MOA) developed between DHS and the CSPs are based on approved templates that have been fully coordinated through the program manager, system owner, Office of the General Counsel, and NPPD Office of Privacy. The relationship between CSPs and ECS participants will be governed through commercial agreements. CS&C is not a party to those agreements.

Responsible Officials

Brendan Goode
Director, Network Security Deployment
Office of Cybersecurity and Communications
National Protection and Programs Directorate
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security

Appendix 1 - Enhanced Cybersecurity Services for Critical Infrastructure

Critical infrastructure (CI) are the assets, systems, and networks, whether physical or virtual, 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. Attacks on CI could significantly disrupt the functioning of government and business alike and produce cascading effects far beyond the targeted sector and physical location of the incident. Therefore, protecting and ensuring the continuity of the CI of the United States, especially from cyber threats, are essential to the nation's security, public health and safety, economic vitality, and way of life.

The Homeland Security Presidential Directive 7 (HSPD-7) established U.S. policy for enhancing CI protection by establishing a framework for the Department's partners to identify, prioritize, and protect the CI in their communities from terrorist attacks. The directive identified 17 CI sectors and, for each sector, designated a federal Sector-Specific Agency (SSA) to lead protection and resilience-building programs and activities. HSPD-7 allows for the Department of Homeland Security to identify gaps in existing CI sectors and establish new sectors to fill these gaps. Under this authority, the Department established an 18th sector, the Critical Manufacturing Sector, in March 2008.

The eighteen CI sectors[17] are:

- Food and Agriculture
- Commercial Facilities
- Dams
- Energy
- Information Technology
- Postal and Shipping
- Banking and Finance
- Communications
- Defense Industrial Base
- Government Facilities
- National Monuments and Icons
- Transportation Systems
- Chemical
- Critical Manufacturing
- Emergency Services

[17] More information about the eighteen CI sectors, the responsible Sector-Specific departments and agencies, and dependencies between the sectors, can be found at: http://www.dhs.gov/critical-infrastructure-sectors

- Healthcare and Public Health
- Nuclear Reactors, Materials, and Waste
- Water

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu