Privacy Impact Assessment Update
for the

Enhanced Cybersecurity Services (ECS)

DHS/NPPD/PIA-028(a)

November 30, 2015

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

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

Abstract

Enhanced Cybersecurity Services (ECS) is a voluntary program that shares indicators of malicious cyber activity between the Department of Homeland Security (DHS) and participating Commercial Service Providers (CSPs) and Operational Implementers (OIs). The National Protection and Programs Directorate (NPPD) is conducting this Privacy Impact Assessment (PIA) Update to reflect ECS' support by Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, announce the expansion of service beyond Critical Infrastructure sectors to all U.S.-based public and private entities, and to introduce the new Netflow Analysis service.

Overview

Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* issued on February 12, 2013 directed federal departments and agencies to work together and with the private sector to strengthen the security and resilience of the Nation's critical infrastructure. Specifically, Section 4(c) of the Order supported DHS's Enhanced Cybersecurity Services (ECS) effort and as services were expanded to all 16 U.S. Critical Infrastructure (CI) sectors. Enhanced Cybersecurity Services (ECS) is a voluntary program that shares indicators of malicious cyber activity between the Department of Homeland Security (DHS) and participating Commercial Service Providers (CSPs)[1] and Operational Implementers (OIs).[2]

As a result of ongoing, high-profile cyberattacks and the increased sophistication of our adversaries, DHS has continued to expand ECS beyond CI entities to include all U.S.-based public and private entities. The description of the program articulated in the January 2013 PIA remains unchanged by the EO, and DHS continues to share indicators of malicious activity (known as Government Furnished Information (GFI)) with approved CSPs and OIs. The CSPs use GFI to protect their ECS customers who are U.S.-based public and private entities.

Netflow Analysis

ECS remains a voluntary program, and with the expansion, allows for enhanced protection of all U.S.-based public and private entities that choose to participate in the program. The initial implementation of ECS involved two cyber threat[3] services: 1) DNS Sinkholing and

[1] Commercial Service Provider (CSP) is a public or private company that has sufficient technical and security capabilities to implement ECS system protections. Once accredited by DHS, a CSP can offer ECS to U.S.-based public and private entities, in addition to using ECS to protect their own networks and systems.

[2] OIs follow the same security requirements as CSPs, but use GFI to protect only their internal networks.

[3] 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.

2) Email Filtering. [4] ECS will offer further protections to U.S.-based public and private sector entities utilizing GFI with a new service called Netflow Analysis.

Netflow Analysis is meant to provide entities with near real-time actionable alerts based on GFI, which would allow for the mitigation/remediation of incidents that could have otherwise gone unnoticed. This new capability will involve the CSPs working with their customers to receive netflow records from across their enterprise that will show traffic flows and volume. CSPs will then use GFI to detect instances of malicious activity occurring on their customers' networks. The Netflow Analysis service will operate in passive mode and will not be able to automatically modify or block malicious traffic. Like other ECS services, Netflow Analysis can be offered, via CSPs, to subscribing customers as a stand-alone service, without requiring the CSP to serve as a customer's Internet Service Provider (ISP). Netflow Analysis will be available on a strictly voluntary basis, with CSP/OI partners responsible for implementation.[5] DHS previously described the use of GFI for services in the ECS PIA (published on January 16, 2013), along with the opportunity that CSPs may, with the permission of the participating entity, also provide limited, anonymized, and aggregated, cybersecurity metrics information to DHS sufficient to understand the performance of the ECS program, including the effectiveness of an indicator in preventing an associated known or suspected cyber threat. CSPs may also voluntarily provide CS&C with lessons learned or other general feedback about ECS technical or operational issues and solutions. The addition of Netflow Analysis as a service does not change this limited voluntary reporting back to DHS.

As with the other services, Netflow Analysis is not meant to replace any existing security offerings operated by or available to protected entities. ECS, including the new Netflow Analysis capability, does not involve government monitoring of any private networks or communications. Based on the effectiveness of the program and the evolution of the threat, DHS may add additional services to ECS, and will continue to monitor any changes to potential collection and use of Personally Identifiable Information (PII).

Reason for the PIA Update

The existing PIA for Enhanced Cybersecurity Services (ECS) was published on January 16, 2013. This ECS PIA update highlights EO 13636, which supported DHS's effort to expand

Information about cyber threats may be received from government, public, or private sources. Categories of cyber threats may include: phishing, Internet Protocol spoofing, botnets, denials of service, distributed denials of service, man-in-the-middle attacks, or the insertion of other types of malware.

[4] CS&C is phasing out the use of the term countermeasures (as reflected in the January 2013 PIA) for ECS, and will instead reference DNS Sinkholing, E-mail Filtering, and Netflow Analysis as "services."

[5] Due to the CSPs/OIs being responsible for the ECS services on their respective networks/systems, the responsibilities for information security and the role of the Information System Security Officer(s) (ISSO) would also be with the CSPs/OIs.

ECS to all 16 CI sectors in 2013. This update also introduces a new service, Netflow Analysis, and addresses ECS expansion beyond CI sectors to all U.S.-based public and private entities.

Additionally, this PIA Update addresses the four (4) recommendations from the April 15, 2015, DHS Privacy Compliance Review (PCR) of the ECS Program: [6]

1. Provide updated information about indicator retention
2. Reflect the current state of testing and the existing data quality protections;
3. Reflect the current frequency of log reviews; and
4. Describe how its subsequent analysis of cybersecurity metrics may lead to the development of new indicators.

Finally, because the ECS PIA was finalized in 2013, this update helps clarify certain aspects of program operations. ECS has not changed how it operates, but NPPD has implemented process improvements and refined guidance documents.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

EO 13636 (dated February 2013) is an additional authority that supports the ECS scope and mission. This PIA update does not change how the relationship between CSPs/OIs and DHS are governed.

Characterization of the Information

DHS collects cyber threat information in the form of indicators (known as GFI), from a variety of Government sources. The initial ECS PIA incorrectly stated that indicators are tested for false positives and false negatives before sharing with the CSPs. While testing is a part of the signature development lifecycle as it relates to DHS' deployment of signatures to the .gov domain, ECS shares indicators (GFI) with a CSP or OI. Indicators serve as the basis for an entity to develop a signature and in the ECS context; the CSP or OI may choose to use GFI to develop signatures and would follow its own processes for testing. Consequently, because DHS is sharing indicators for ECS, not signatures, indicator testing is not performed.

[6] http://www.dhs.gov/sites/default/files/publications/privacy-pcr-ecs-04102015.pdf

GFI is shared and stored with CSPs and OIs via secure channels. CSPs use the GFI to protect their customers who are U.S.-based public and private entities, while OIs use GFI to protect their own internal network. Given the voluntary nature of the program, CSPs can choose to develop signatures on their own, using GFI, and CSPs are not required to use all the GFI. The GFI shared is governed by the program's GFI Data Verification and Vetting Process and is timely, actionable, and vetted by DHS.

DHS shares 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. Please note that, as stated in the PCR, the CSPs currently report back a subset of the information listed as being allowable in the ECS Memorandum of Agreement (MOA). This information is limited to Reference ID, date, time, and the service to which the activity is attributed. Due to the limitations of data received back, no indicators are currently derived from metric data.

All ECS indicators are stored via secure channels. In addition, unclassified indicators for ECS are stored on the unclassified Cyber Indicators and Analysis Platform (CIAP) and on the NCPS Mission Operating Environment (MOE).

Uses of the Information

CS&C provides cybersecurity indicators to CSPs/OIs for the purpose of enhancing the protection of ECS participant networks. The CSPs/OIs, at the request of ECS participants, use indicators to block known or suspected cyber threats. As part of the program, the CSPs/OIs may share summary information with CS&C about the fact that known or suspected cyber threats were detected. This "fact of" occurrence reporting does not contain information that could be considered PII. This summary feedback 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 have the same privacy protections as those included in all indicator development.

The addition of Netflow Analysis to ECS does not introduce additional privacy risks;no PII is collected for Netflow Analysis.

Notice

This PIA Update serves as general notice for the addition of Netflow Analysis to 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: http://www.dhs.gov/cybersecurity-and-privacy.

All authorized users of the participating U.S.-based entity's network are notified via an electronic login banner, or other written notification, 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 to the public that the agency uses computer security programs to monitor network traffic.

Government users inside the agency network receive notice from their agency's logon banners and user agreements that communications and transiting data are stored on the agency network and that network traffic is subject to monitoring and disclosure for network security and other lawful government purposes.

Data Retention by the project

The National Archives and Records Administration approved a records retention schedule for the National Cybersecurity Protection System (NCPS) on January 12, 2015.[7] The NCPS Records Retention Schedule is broken down into five broad capability areas and covers all fields and data collected by and maintained on NCPS, including the voluntary metric information for ECS. 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.

Information Sharing

No change from previous PIA

Redress

No change from previous PIA

Auditing and Accountability

The Memoranda of Agreements (MOAs) developed between DHS and the CSPs/OIs 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. Commercial agreements continue to govern the relationship between CSPs/OIs and ECS participants.

[7] Record Schedule DAA-0563-2013-0008. A link to the approved schedule is here: http://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/daa-0563-2013-0008_sf115.pdf.

CSPs/OIs can update those Commercial agreements to include Netflow Analysis as an available service. CS&C is not a party to those agreements.

In addition to the governance and oversight described in the 2013 ECS PIA and above, this program also underwent a DHS PCR published in April 2015. The PCR found 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 risk as the program evolves and matures."[8] The recommendations from the PCR report reflected "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."[9] One recommendation from the PCR was that NPPD clarify the frequency of its log reviews from what is stated in the January 2013 ECS PIA. Accordingly, NPPD clarifies that NCPS user account activity is logged, and the logs are reviewed regularly.

Responsible Official

Andy Ozment
Assistant Secretary, Office of Cybersecurity and Communications
National Protection and Programs Directorate
Department of Homeland Security

Approval Signature

Original signed copy on file with DHS Privacy Office.

____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

[8] *See* Page 5 of the Privacy Compliance Review of the Enhanced Cyber Security Services Program, dated April 10, 2015. Available at: http://www.dhs.gov/sites/default/files/publications/privacy-pcr-ecs-04102015.pdf.

[9] *See* Page 5 of the Privacy Compliance Review of the Enhanced Cyber Security Services Program, dated April 10, 2015. Available at: http://www.dhs.gov/sites/default/files/publications/privacy-pcr-ecs-04102015.pdf.