Privacy Impact Assessment Update
for the

Joint Cybersecurity Services Program (JCSP), Defense Industrial Base (DIB) – Enhanced Cybersecurity Services (DECS)

DHS/NPPD/PIA-021(a)

July 18, 2012

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

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

Abstract

The Joint Cybersecurity Services Pilot (JCSP) is the Department of Homeland Security's (DHS) voluntary information sharing initiative with the Department of Defense (DOD) and participating commercial companies. The National Protection and Programs Directorate (NPPD) is updating the DHS/NPPD/PIA-021 National Cyber Security Division Joint Cybersecurity Services Pilot PIA published on January 13, 2012 to reflect the establishment of the JCSP as an ongoing permanent program (now known as the Joint Cybersecurity Services Program (JCSP)). The purpose of the program is to enhance the cybersecurity of participating critical infrastructure entities through information sharing partnerships with the critical infrastructure organization or their Commercial Service Provider (CSP). The first phase of the JCSP will focus on the cyber protection of the Defense Industrial Base (DIB) companies that are participating in the DoD's Cyber Security/Information Assurance (CS/IA) Program. This sub-program is known as the DIB Enhanced Cybersecurity Services (DECS). The JCSP may also be used to provide equivalent protection to participating Federal civilian agencies pending deployment of EINSTEIN intrusion prevention capabilities.

Overview

Under the Joint Cybersecurity Services Pilot, DHS, through the National Cyber Security Division's (NCSD) U.S. Computer Emergency Readiness Team (US-CERT), partnered with the DOD to share cyber threat indicators and other information about known or suspected cyber threats directly with voluntary partners from the DIB sector and their CSPs. The pilot was commissioned for 180 days and during that time met its goal to effectively share cyber-related information with CSPs for cybersecurity purposes. With the expiration of 180 days, DHS established the pilot as an ongoing voluntary program (now known as JCSP). The first phase of the JCSP will focus on the cyber protection of the DIB companies that are participating in the DOD's CS/IA Program.[1] This sub-program is known as the DECS. The JCSP may also be used to provide equivalent protection to participating Federal civilian agencies pending deployment of EINSTEIN intrusion prevention capabilities.

[1] DoD leverages its DoD DIB Cyber Security/Information Assurance Activities PIA (http://dodcio.defense.gov/Portals/0/Documents/DIB%20CS-IA%20PIA_FINAL_signed_30jun2011_VMSS_GGMR_RC.pdf?) and established procedures and agreements with DIB participants.

Initially under the pilot and now under DECS, US-CERT reviews information that is specific to identifying known or suspected cyber threats that is obtained from a number of sources in the form of "indicators" (e.g., Internet Protocol (IP) addresses, domains, e-mail headers, files, and strings). US-CERT then shares that information with participating CSPs through secure communication channels. The CSPs configure the indicators into "signatures,"[2] which are machine-readable software code that enable automated detection of the known or suspected cyber threats associated with the indicators.

When CSPs implement a signature for the benefit of the participating DIB company and that signature triggers an alert, the CSP notifies the participating DIB company in accordance with its commercial agreement and any applicable security requirements. The CSP may, with the permission of the participating DIB company, provide the fact of an incident to US-CERT, including the signature that triggered the alert. The CSP may, with the permission of the participating DIB company provide some limited information about the alert to US-CERT. US-CERT may share the "fact of occurrence" of the alert with DOD. Additionally, CSPs may voluntarily choose to send US-CERT their own information related to cyber threat indicators or other possible known or suspected cyber threats.

When a CSP implements a signature for the benefit of the participating federal civilian agency and that signature triggers an alert, the CSP reports both the fact of occurrence and the additional details regarding the incident to US-CERT. The nature of the reporting is consistent with data collected and analyzed under the DHS EINSTEIN[3] efforts and agency responsibilities under the Federal Information Security Management Act for securing federal agency information systems.

Reason for the PIA Update

The DHS/NPPD/PIA-021 National Cyber Security Division Joint Cybersecurity Services Pilot PIA was published on January 13, 2012. NPPD is updating the JCSP PIA to reflect the successful completion of the pilot and the establishment of the JCSP as an ongoing voluntary program and to describe the first phase as DECS.

---

[2] More information about the JCSP, and how signatures are used for the JCSP DECS, is addressed in the Privacy Impact Assessment for the National Cyber Security Division Joint Cybersecurity Services Pilot that was published on January13, 2012, and can be found at: http://www.dhs.gov/files/publications/gc_1284567214689.shtm#15.

[3] Related Privacy Impact Assessments for the EINSTEIN Program can be found at: http://www.dhs.gov/files/publications/editorial_0514.shtm#4.

Privacy Impact Analysis

Authorities and Other Requirements

DHS's effort in connection with DECS is being conducted pursuant to authority derived from the Homeland Security Act, including 6 U.S.C. §§ 121, 143; 10 U.S.C. § 2224; the Federal Information Security Management Act, including 44 U.S.C. § 3544; Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*; and Homeland Security Presidential Directive 23, *Cybersecurity Policy*. There are agreements in place between DHS and the CSPs as well as between DoD and participating DIB companies. The relationship between CSPs and participating entities will be governed through contracts between the CSP and participating entity.

Personally identifiable information (PII) submitted to US-CERT by individuals in order to verify any reported known or suspected cyber threats, and to follow up for additional action that may be required regarding the particular cyber threats or any other aspect of DECS 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. The review and receipt of information about indicators or other information related to a known or suspected cyber threat, does not constitute a "system of record" under the Privacy Act because information is not retrieved by a personal identifier and therefore, no system of records notice applies.

US-CERT maintains signatures and related cyber threat information obtained through DECS in the National Cybersecurity Protection System (NCPS) Mission Operating Environment (MOE), which has a completed system security plan.

The Department is working with NPPD Records Manager to develop a disposition schedule. Once completed, the schedule will be sent to the National Archives and Records Administration for approval.

The Paperwork Reduction Act does not apply to DECS.

Characterization of the Information

DECS has not changed the source of information, the use of commercial information, and the accuracy of the information used under JCSP. No new privacy risks have been identified.

US-CERT obtains contact information from representatives of DECS participants, to include employee name, business address, business telephone number and business email address. This information is used by US-CERT to verify any reported known or suspected cyber threats and to follow up for additional action that may be required.

Under this program, US-CERT may also receive and review indicators and other cyber threat related information, which may include PII such as email address, information from and associated with email headers and email.

US-CERT receives indicators and other cyber threat related information from a number of sources including the following: analysis by US-CERT's operations teams; data submitted to US-CERT from other government departments and agencies; and reports received from mission and industry partners. Indicators can be parsed as received reports and submitted by analysts from US-CERT and other government departments/agencies or from information received by mission and industry partners, including the EINSTEIN efforts. Under DECS, US-CERT also accepts indicators from DOD and provides cyber indicators and alerting information back to DoD.

US-CERT can use information from a range of sources, including commercial sources and publicly available data on cybersecurity threats. As an example, indicator information obtained from WHOIS[4] can be used to help resolve cybersecurity-related threats and for historical reference of similar threats.

Both classified and unclassified indicators are vetted through trusted and validated sources, using unclassified references for indicators whenever possible. The indicators are tested for false positive and false negative results in a pre-staged, EINSTEIN test sensor before they are provided to the CSPs. Further, additional testing is performed in the production environment to test for true positive and true negative results.

There is a risk that information that could be considered PII is included in an indicator and that the indicator does not add any value to the prevention of a known or suspected cyber threat. US-CERT has policies and procedures in place to ensure the quality and integrity of indicators and procedures for ensuring the proper minimization, protection, and disclosure of PII. Only information determined to be directly relevant and necessary to accomplish the specific purpose of the program will be retained; otherwise, the data is deleted. US-CERT will conduct periodic reviews of cyber indicators to ensure all standards and responsibilities are met.

---

[4] WHOIS is a Transmission Control Protocol (TCP)-based transaction-oriented query/response protocol that is commercially available and 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. (http://www.ietf.org/rfc/rfc3912.txt). DHS subscribes to and receives commercially/publicly available WHOIS information which includes: person and organization names, addresses, emails, phone numbers, contact information (address, email, phone) for both administrative contacts as well as technical contacts. The Internet Corporation for Assigned Names and Numbers (ICANN) is the keeper of the WHOIS database and each of the domain providers who register domains with ICANN WHOIS service must be informed that the data is public, and users have no reasonable expectation of privacy.

Uses of the Information

DECS does not change the uses of information under JCSP. No new privacy risks have been identified.

DECS is a voluntary program based on mutual sharing of information. US-CERT provides indicators of known or suspected cyber threats to CSPs for the purpose of enhancing the protection of DECS participants. The CSPs, at the request of participants, in turn use such indicators to look for known or suspected cyber threats in the traffic to or from the DECS participant's network. As part of DECS, the CSP may, with the permission of the participating DIB company, also provide some limited information about the incident to US-CERT sufficient to capture the fact of occurrence. This data will not contain information that could be considered PII.

DECS 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.

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

The privacy impact of DECS is that indicators of known or suspected cyber threats collected and disclosed may contain PII that is not necessary to the mitigation of the cyber threat. Those individuals whose PII is incidental to a known or suspected cyber threat may not understand how their information may be used. US-CERT has established policies and procedures for developing indicators and removing PII that is unnecessary to address the cyber threat.

Notice

This Update PIA serves as notice of DECS. Notice has also been provided through the initial January 13, 2012 publication of the DHS Joint Cybersecurity Services Pilot PIA, on which DECS is based. 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.

Data Retention by the project

DECS does not change the data retention requirements under JCSP. Given DECS has moved into an ongoing program there is no termination date at which point voluntary DECS participants must return government furnished information back to the government.

DHS is currently working to determine the appropriate length of time for cyber indicators and related information, including PII identified as related to malicious activity to be retained and stored.

The Department is currently working with the NPPD Records Manager to develop a disposition schedule. Once completed, the schedule will be sent to the National Archives and Records Administration for approval.

DHS will retain DECS information following National Directives and DHS standards for data retention to enhance the cybersecurity of participating DIB critical infrastructure entities and to protect sensitive DOD information residing on or passing through DIB systems. Minimal retention reduces the amount of information vulnerable to unauthorized use or disclosure.

Information Sharing

DECS does not change the internal and external sharing and disclosure under JCSP. Under the DECS, US-CERT shares indicators with CSPs and DOD for the purpose of enhancing the protection of the DECS participants. The sharing of information between the parties is accomplished through secure communication.

Contact information from representatives from the DIB companies, the CSPs and the participating federal agencies will not be shared outside the normal agency or DECS operations.

No new privacy risks have been identified.

Redress

DECS does not change the opportunities for access, redress, and correction under JCSP. For information submitted directly by individuals in order to verify any reported known or suspected cyber threats, individuals may seek access to any records containing information that is part of a DHS system of records or seeking to amend the accuracy of its content may submit a Freedom of Information Act (FOIA) or 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.

Given the nature of some information in the US-CERT systems, DHS may not always permit the individual to gain access to or request amendment of his or her record.

No new privacy risks have been identified.

Auditing and Accountability

DECS does not change the auditing and accountability procedures that governed JCSP.

The US-CERT Oversight and Compliance Officer will ensure adequate guidelines and procedures are in place and that all US-CERT personnel working in support of DECS are familiar with, understand and adhere to those guidelines. The US-CERT Oversight

and Compliance Officer will conduct quarterly internal reviews to evaluate the program and assess its compliance with applicable guidelines, procedures, and applicable laws and regulations.

All DHS employees 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 are also required to complete annual Security Education and Awareness Training (SEAT). In addition, US-CERT analysts and other persons who might come into contact with sensor or other data receive annual training on privacy, legal, and policy issues specifically related to US-CERT operations. This training includes how to address privacy during the development of new signatures, 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. In addition NCSD is in the process of developing training specifically for analysts supporting DECS.

Access to US-CERT systems is restricted to individuals with demonstrated need for access, and such access must be approved by the supervisor as well as the NCSD Information System Security Officer. 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. 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.

The Agreements developed between DHS and the CSPs, are coordinated through the program manager, system owner, Office of the General Counsel and NPPD Office of Privacy. The relationship between CSPs and JCSP participants will be governed through commercial transactions.

Responsible Official

Brendan Goode
Director, Network Security Deployment
National Cyber Security Division
National Protection and Programs Directorate
Department of Homeland Security

Approval Signature

_____

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security