Assistant Secretary for Legislative Affairs
U.S. Department of Homeland Security
Washington, DC 20528

DEC 0 3 2010

Homeland Security

The Honorable John McCain
Ranking Member
Committee on Armed Services
United States Senate
Washington, DC 20510

Dear Senator McCain:

This letter sets forth the views of the Department of Homeland Security (DHS) on S. 3454, the "National Defense Authorization Act for Fiscal Year 2011," as reported by the Committee on Armed Services.

One of DHS's primary missions is to lead a coordinated national effort to secure federal civilian agency, state, local, tribal, territorial, and private sector networks. DHS has a clear mandate to collaborate with the private sector to promote and improve the security of non-federal government systems during steady-state operations and in times of crisis. Congress and the President have assigned DHS important responsibilities for coordinating the protection of critical infrastructure from cyber and physical threats. Similarly, they have assigned the Department of Defense (DoD) important responsibilities for the protection of DoD information and defense information infrastructure. Within the construct of the National Infrastructure Protection Plan (NIPP) and Homeland Security Presidential Directive 7 (HSPD-7), DoD is the Sector Specific Agency (SSA) for Defense Industrial Base (DIB) critical infrastructure protection activities undertaken in coordination with DHS. The coordinated and collaborative activities of DoD and DHS in their respective areas of responsibility are vital to the nation's security, military readiness, and the Government's overall efforts to improve cybersecurity.

S. 3454 contains provisions that may impede, duplicate or otherwise confuse these authorities, responsibilities and roles already assigned to DHS and DoD through statute and policy. DHS therefore urges the Senate to address the following concerns:

- ***Sec. 215 (Demonstration and Pilot Projects on Homeland Security)*** — The pilot program proposals identified in section 215 do not necessarily reflect the cybersecurity priorities of the Executive Branch in general, or of the Departments of Homeland Security or Defense in particular. In addition, DHS and DoD have not had a sufficient opportunity for coordination or research to determine whether the proposed pilots are technologically feasible, or whether they will result in an efficient use of finite government resources. Finally, the pilot program proposals do not fully reflect the roles and authorities of DHS and other federal departments in the coordinated cybersecurity activities of the Government.

In contrast, the Senate Report (S. Rep. No. 111-188) accompanying the Supplemental Appropriations Act, 2010 (Pub. L. 111-212) provided DoD and DHS far greater flexibility in pilot program activity, and underscored the expectation for appropriate interagency coordination on joint pilot program efforts. DHS believes that the broad approach taken in the report is more appropriate than that proposed in the current version of S. 3454. If a similarly broad approach cannot be adopted here, however, DHS offers the following additional comments:

- Sec. 215(a)(2) (Scope of Projects) — Although this provision calls for demonstration projects to align with current Executive Branch priorities such as the Cyberspace Policy Review and the Comprehensive National Cybersecurity Initiative (CNCI), it fails to acknowledge key cybersecurity mission leaders, such as DHS, identified in those critical cyber policy statements. Significant work is already underway within DHS and other agencies in furtherance of the CNCI goals. Initiating additional projects that are not coordinated with these efforts could have the effect of disrupting or delaying ongoing efforts, and could result in the development of competing, not complementary, approaches to widespread cybersecurity challenges. In order to ensure that consistent, repeatable, and leveraged solutions are being developed across the interagency, we recommend that this subsection be amended to explicitly identify DHS as a co-lead in all demonstration project activity. This change would ensure appropriate coordination and deconfliction between DHS and DoD's cybersecurity missions and activities in accordance with existing agency roles and responsibilities.

- Sec. 215(b)(2) (Threat Sensing and Warning for Information Networks Worldwide) — DHS has significant concerns about the implicit direction for DHS to establish a consortium of telecommunications service providers, Internet service providers and other private sector entities. First, DHS has not determined that establishing such consortium is consistent with departmental priorities or Government-wide cybersecurity priorities. Second, the establishment of a consortium of selected private sector entities may implicate a range of antitrust, unfair competition, or other legal concerns that will have to be fully considered. Third, DHS has not yet determined whether it has sufficiently clear authority or the necessary funding to carry out all of the efforts associated with creating such a consortium.

- Sec. 215(b)(3) (Managed Security Services for Cybersecurity within Defense Industrial Base) — Any pilot program established under this provision must account for parallel activity underway at DHS involving public and private sector partners at the National Cybersecurity and Communications Integration Center and under the National Cyber Incident Response Plan. The section should also build upon, and not confuse, existing public-private relationships under HSPD-7 and the NIPP Partnership Framework. DHS is responsible for engaging with private sector companies, including those within the DIB. Therefore, any DoD activity to offer managed security services to the DIB

should be done in partnership with DHS, so as to best leverage DHS's efforts in the field and not give duplicative or inconsistent direction to the private sector.

- Sec. 215(b)(4)-(5) — These provisions fail to account for DHS's role in securing federal civilian systems and coordinating the protection of critical infrastructure. They should be amended to explicitly identify DHS as a co-lead on coordinating the ongoing work of DoD and DHS with respect to the private sector, as well as the joint efforts of DHS and the General Services Administration to develop strategic sourcing contract vehicles for federal agencies.

- ***Sec. 931(Continuous Monitoring of Department of Defense Information Systems for Cybersecurity)*** — DHS is concerned that this provision fails to fully reflect DHS's authority to coordinate the protection of critical infrastructure across all sectors, including the DIB. The Department is also concerned that the "automation of continuous monitoring" provision in section 931(a)(2) may conflict with agency reporting requirements under the Federal Information Security Management Act (FISMA) and current Office of Management and Budget guidance. Moreover, use of the term "information infrastructure of the Department of Defense" in subsection (a)(2) may create confusion with respect to other categories of systems outlined in FISMA and other statutes. Therefore, the Department recommends that "information infrastructure of the Department of Defense" be replaced with "Department of Defense agency systems (as such term is described in 44 U.S.C. 3543(c)(2))". In addition, two technical and conforming changes would be necessary to section 931: (A) changing the reference in subsection (a)(2) from "of that infrastructure" to "of that category of systems"; and (B) deleting the definition of "information infrastructure" in subsection (b)(2).

- ***Sec. 935 (Reports on Department of Defense Progress in Defending the Department and the Defense Industrial Base from Cyber Events)*** — This provision could be construed as giving DoD direct authority to defend the DIB from cyber events beyond existing DoD authority under the Defense Information Assurance Program (10 U.S.C. § 2224). Any such expansion of DoD authority with respect to the private sector should reflect the clear role for DHS set out in Title II of the Homeland Security Act (6 U.S.C. 121 et. seq.) and existing Executive Branch directives. At minimum, this provision should be amended to explicitly recognize this role by replacing the existing language with the following: "Not later than March 15, 2011, and every year thereafter through 2015, the Secretary of Defense shall submit to the congressional defense committees a report on the progress of the Department of Defense in defending the Department, and the Department's joint progress with the Department of Homeland Security in protecting the defense industrial base from cyber events (such as attacks, intrusions, and theft)."

In addition to the concerns identified in sections 215, 931, and 935 of S.3454, DHS would also oppose any attempt by the Senate to include provisions identical or similar to language in title XVII of H.R. 5136, the "National Defense Authorization Act for Fiscal Year 2011," as passed by

the House of Representatives. Title XVII (Federal Information Security) would inappropriately assign operational authorities and responsibilities for securing Federal civilian and domestic private sector networks to the Executive Office of the President that are more appropriately located in DHS. The reassignment of such authorities and responsibilities would seriously disrupt the operation and management of cybersecurity programs, and would contradict DHS's primary mission to lead a coordinated national effort to secure federal civilian agency, state, local, tribal, territorial, and private sector networks.

The Department looks forward to working with the Senate to address these and other concerns with S. 3454.

The Office of Management and Budget advises that, from the standpoint of the Administration's program, there is no objection to the presentation of these views to Congress.

An identical letter has been sent to Chairman Carl Levin.

I appreciate your interest in the Department of Homeland Security, and I look forward to working with you on future homeland security issues. If I may be of further assistance, please contact me at (202) 447-5455.

Sincerely,

Nelson Peacock
Assistant Secretary
Office of Legislative Affairs

Privacy Impact Assessment
for the

National Cyber Security Division
Joint Cybersecurity Services Pilot (JCSP)
DHS/NPPD-021

January 13, 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 Department of Homeland Security (DHS) and the Department of Defense (DoD) are jointly undertaking a proof of concept known as the Joint Cybersecurity Services Pilot (JCSP). The JCSP extends the existing operations of the Defense Industrial Base (DIB) Exploratory Cybersecurity Initiative (DIB Opt-In Pilot) and shifts the operational relationship with the CSPs in the pilot to DHS. The JCSP is part of overall efforts by DHS and DoD to enable the provision of cybersecurity capabilities enhanced by U.S. government information to protect critical infrastructure information systems and networks. The purpose of the JCSP is to enhance the cybersecurity of participating DIB critical infrastructure entities and to protect sensitive DoD information and DIB intellectual property that directly supports DoD missions or the development of DoD capabilities from unauthorized access, exfiltration, and exploitation. The National Protection and Programs Directorate (NPPD) is conducting this Privacy Impact Assessment (PIA) on behalf of DHS because some known or suspected cyber threat information shared under the JCSP may contain information that could be considered personally identifiable information (PII).

Overview

The Joint Cybersecurity Services Pilot (JCSP) 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 (FISMA), 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*.

During the Defense Industrial Base (DIB) Exploratory Cybersecurity Initiative (DIB Opt-In Pilot),[1] DoD shared classified indicators associated with cyber threat countermeasure[2] capabilities directly with commercial service providers (CSPs)[3] in order to protect information on DIB company networks. The DIB Opt-In Pilot focused on two cyber threat countermeasures: 1) the ability to block Domain Network System (DNS) traffic to malicious domains (referred to as DNS Sinkholing), and 2) e-mail filtering that would include quarantining incoming infected messages. The JCSP seeks to build upon the DIB Opt-In Pilot and allow DHS, through the National Cyber Security Division (NCSD) U.S. Computer Emergency Readiness Team (US-CERT), to share indicators and other information about known or suspected cyber threats

[1] The DoD DIB Opt-in Pilot leveraged the DoD DIB Cyber Security /Information Assurance Activities PIA (at http://dodcio.defense.gov/docs/DIB%20CS-IA%20PIA_FINAL_signed_30jun2011_VMSS_GGMR_RC.pdf) and established procedures and agreements with DIB participants.

[2] A countermeasure is an action, process, device, or system that can prevent, or mitigate the effects of, threats to a computer, server or network.

[3] The term Commercial Service Providers, or CSP, refers to internet, network and communications providers.

directly with CSPs to enhance the protection of JCSP participants, including certain DIB companies and any participating federal agencies.

Indicators of Known or Suspected Cyber Threats

As part of its mission to promote the protection of cyber infrastructure, NCSD, through the US-CERT, collects information that is specific to identifying known or suspected cyber threats from a number of sources. These "indicators" can be used to create intrusion detection signatures or other means of detecting and mitigating cyber threats. Sources for indicators may include individuals with expertise, 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 EINSTEIN[4] sensors placed on federal agency network collection points.[5]

US-CERT typically characterizes these indicators into five categories:

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

Each category of indicators contains specific features or characteristics. For instance:

- IP and Domain Indicators can contain the associated port, WHOIS[6] information, and Uniform Resource Identifiers[7] (URI);
- 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, hash values, and behavior; and

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

[5] These sensors capture flow records that identify the Internet Protocol (IP) address of the computer that connects to the federal system, the port the source uses to communicate, the time the communication occurred, the federal destination IP address, the protocol used to communicate, and the destination port.

[6] 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. (http://www.ietf.org/rfc/rfc3912.txt)

[7] 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.

- String Indicators consist of persistent and unique identifiers specific to malicious activity.

NCSD is not a classification authority. Classification of identified indicators is dictated by its source, including the JCSP. However, the majority of information the US-CERT manages and analyzes is unclassified and therefore potentially available for dissemination to a large majority of its mission partners. Classified indicators are managed on secure media and only disseminated within those protected and authorized boundaries. The risk for PII is minimized because US-CERT operates with domain names and simple mail transfer protocol (SMTP) strings, neither of which includes PII.

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

Indicator Sharing Under the JCSP

As part of the JCSP, US-CERT shares indicators with CSPs through secure channels. The CSPs will 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 indicator described above.

The JCSP will use the same two cyber threat countermeasures used in DoD's DIB Opt-in Pilot: 1) DNS Sinkholing and 2) email filtering that would include quarantining infected messages.

When CSPs implement a signature on behalf of a 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, also provide some limited information about the incident to US-CERT sufficient to capture the fact of occurrence. US-CERT may share the fact of occurrence information with DoD pursuant to existing US-CERT procedures in an effort to increase DoD's understanding of the threats to their critical assets that reside within the DIB companies' networks and system. The CSPs may voluntarily choose to send US-CERT information related to cyber threat indicators or other possible known or suspected cyber threats.

When a CSP implements a signature on behalf of a 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. The nature of the reporting will be consistent with data collected and analyzed under the DHS EINSTEIN efforts and agency responsibilities under FISMA for securing federal agency information systems.

US-CERT will share information it receives under JCSP consistent with its existing policies and procedures, including to other U.S. government entities with cybersecurity responsibilities.

US-CERT maintains its information involved in JCSP in the National Cybersecurity Protection System (NCPS) Mission Operating Environment (MOE), a protected system on a protected network accessible to only authorized NCSD personnel with a need to know. JCSP participants and CSPs maintain information in accordance with information sharing agreements. At the end of JCSP, JCSP participants and CSPs must return all government furnished information or dispose of it in accordance with establishing information sharing agreements. They may also voluntarily provide NCSD with end-of-pilot lessons learned or other general feedback about JCSP technical or operational issues and solutions.

Privacy Considerations

The JCSP is a voluntary program based on mutual sharing of cybersecurity information between the U.S. government, service providers, and the organizations being protected by the CSPs. US-CERT provides cybersecurity indicators to CSPs for the purpose of enhancing the protection of JCSP participants. The CSPs, at the request of participants, in turn use such indicators to look for known or suspected cyber threats within JCSP Participant traffic. As part of the JCSP, CSPs may share summary information with US-CERT about the fact that known or suspected cyber threats were detected. This "fact of" information will not contain PII. When the JCSP ends and NCSD solicits feedback on the project, NCSD will not collect PII.

Participants in the JCSP have determined that their policies, practices, and activities related to the JCSP comply with applicable legal requirements and include measures that the participants determined are sufficient to ensure authorized user consent to the interception, monitoring, access, use and disclosure of electronic communications or data residing on or transiting their systems, including the disclosure of related information to the U.S. government.

Indicators of known or suspected cyber threats that are shared as part of the JCSP may contain information that could be considered PII, such as e-mail addresses and other information that might be included in the message header or subject line. This type of information would only be shared if it was reviewed and pre-determined to be an indicator of a known or suspected cyber threat. All information that could be considered PII is handled in accordance with existing US-CERT standard operating procedures (SOPs), which describe the necessary procedures, defines the terms and outlines roles and responsibilities.

US-CERT collects contact information from representatives of the DIB companies, the CSPs, and federal agencies participating in the JCSP. This information is used by US-CERT during the pilot 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 the operation of the pilot.

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?

The JCSP 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 commercial transactions.

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, US-CERT 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 record by a personal identifier does the Privacy Act require a SORN. US-CERT does not retrieve this information by personal identifier, thus a SORN is not required for the JCSP.

US-CERT collects the contact information from representatives of the DIB companies, the CSPs, and federal agencies participating in the JCSP. This information is used by US-CERT during the pilot to verify any reported known or suspected cyber threats and to follow up for additional action that may be required regard the particular cyber threats, or any other aspect of the operation of the pilot. 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?

JCSP information will be stored in the NCPS MOE, which is the network designated to perform threat analysis and other functions. For the JCSP, US-CERT 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.

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

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.

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.

DHS is not using a form to collect the same information from 10 or more persons, therefore the PRA does not apply.

Section 2.0 Characterization of the Information

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

The JCSP is a voluntary program based on mutual sharing of indicators of known or suspected cyber threats and reporting of incidents of detected cyber threats. US-CERT provides indicators to CSPs for the purpose of enhancing the protection of JCSP participants. The CSPs, at the request of participants, in turn use such indicators to look for known or suspected cyber threats within the traffic to or from JCSP Participant computer networks. As part of the JCSP, 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 "fact of" reporting will not contain information that could be considered PII.

The following information that could be considered PII may be part of indicators shared through the JCSP: email 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 JCSP participants' networks and systems. US-CERT will review all information it receives during the JCSP and only retain information that could be considered PII if that information is analytically relevant, otherwise, US-CERT will delete it.

As part of the JCSP, US-CERT collects contact information from representatives of JCSP Participants, to include employee name, business address, business telephone number, and business email address. This information is used by US-CERT during the pilot 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 the operation of the pilot.

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 US-CERT 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. The JCSP will also allow US-CERT to accept indicators from DoD and provide cyber indicators and alerting information back to DoD.

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

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 can be used to help resolve cybersecurity-related threats and for historical reference of similar threats.

2.4 Discuss how accuracy of the data is ensured.

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.

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: US-CERT only collects data that is necessary to accomplish its mission; cyber threat (i.e., indicator) information may include IP and host addresses and flow data, and any actions taken.

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.

US-CERT will conduct periodic reviews on cyber indicators to ensure all standards and responsibilities are met.

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

Mitigation: US-CERT 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. US-CERT analysts conduct analysis on all cyber threats received. If information submitted contains information that could be considered PII, the analyst must determine if that information is related to the cyber threat. If the information is not related to the cyber threat, it is deleted.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The JCSP 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 protecting of JCSP 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 JCSP Participant's network. As part of the JCSP, 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 information 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; the JCSP 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 JCSP.

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: DHS will not directly receive PII from the CSP and would only receive PII from the participating entities if those entities share it in connection with a known or suspected cyber threat. Aspects of the JCSP are governed by information sharing agreements, internal US-CERT SOPs, and this PIA, which covers the uses of government furnished information, including indicators, collected or maintained.

In addition, DIB companies are bound by established information sharing agreements, or contractual relationships established between the DIB companies and their respective CSPs.

US-CERT analysts supporting the JCSP are trained on both DHS and US-CERT 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, US-CERT maintains SOPs which describe necessary procedures, defines the terms and outlines roles and responsibilities for handling PII.

In addition, 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.

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 notice of the JCSP. Notice is also provided through DoD's published PIA on DoD's DIB Cyber Security and Information Assurance program, which the DoD DIB Opt-in Pilot leveraged. This PIA covers the JCSP overall pilot process and previously published

PIAs that support the overall US-CERT program. 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.

Participants in the JCSP have determined that their policies, practices, and activities related to the JCSP comply with applicable legal requirements and include measures that the participants determined are sufficient to ensure authorized user consent to the interception, monitoring, access, use and disclosure of electronic communications or data residing on or transiting their systems, including the disclosure of related information to the U.S. government.

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

Federal agencies are required to post notices on their websites as well as at other major points of entry that computer security information is being collected and their system monitored. Furthermore, users of federal computer systems are provided with logon banners and sign user agreements that specifically notify them of the computer network monitoring. 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.

Participants in the JCSP have determined that their policies, practices, and activities related to the JCSP comply with applicable legal requirements and include measures that the participants determined are sufficient to ensure authorized user consent to the interception, monitoring, access, use and disclosure of electronic communications or data residing on or transiting their systems, including the disclosure of related information to the U.S. government.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a privacy risk that an individual may choose to not read a notice or banner provided or be aware of the information collection.

Mitigation: Participants in the JCSP have determined that their policies, practices, and activities related to the JCSP comply with applicable legal requirements and include measures that the participants determined are sufficient to ensure authorized user consent to the interception, monitoring, access, use and disclosure of electronic communications or data residing on or transiting their systems, including the disclosure of related information to the U.S. government. Users of federal systems have also been provided notice of, and consented to, network security activities including the potential collection of their communications.

Section 5.0 Data Retention by the Project

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

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.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that PII may be retained beyond what is necessary to appropriately analyze or address a cyber threat or investigation. Additional risks may exist if necessary and appropriate PII is either prematurely deleted or not retained and is pertinent to a cyber threat or investigation.

Mitigation: 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.

US-CERT analysts will only retain indicators associated with known or suspected cyber threats, reports and other products generated as a result of known or suspected cyber threats. JCSP information will be stored in the NCPS MOE, a protected system on a protected network accessible to only authorized NCSD personnel with a need to know the information. In the event information collected does contain PII but it is judged irrelevant to the cyber threat, the PII is deleted in accordance with US-CERT SOPs.

US-CERT maintains SOPs which describe the necessary procedures, defines the terms and outlines roles and responsibilities.

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 the JCSP, US-CERT shares indicators with CSPs and DoD for the purpose of enhancing the protection of JCSP 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.

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

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

Collection of personal information 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. DHS will share this data in a manner that is compatible with the purpose of this systems of records notice.

6.3 Does the project place limitations on re-dissemination?

US-CERT is not prohibited from using or disseminating additional cyber threat indicators, including additional IP addresses or domain names, derived from cybersecurity incident information as long as such indicators do not identify the source of such information and are not otherwise attributable to JCSP Participants.

DIB companies are bound by established information sharing agreements or contractual relationships established between the DIB companies and their respective CSPs.

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

As a general rule, US-CERT provides cyber-related information to the public, federal departments/agencies, state, local, tribal and international entities through a variety of products, many of which are available on the US-CERT.gov website. No formal report contains PII. Each report is numbered and catalogued and references exist in all products (including those associated with indicators shared through the JCSP) 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 with the written approval of the NCSD Director after consultation with the SOPs.

6.5 Privacy Impact Analysis: Related to Information Sharing

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

Mitigation: The risk of unauthorized disclosure is mitigated through various means, including US-CERT standard operating procedures. US-CERT SOPs provide procedures for removing unnecessary PII, encrypting certain information, 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?

Individuals seeking access to any record 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.

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

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

JCSP Participants seeking to correct contact information collected by US-CERT during the JCSP may contact US-CERT operations 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.

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

As part the normal US-CERT operations, US-CERT provides notice about procedures for correcting PII to those individuals that submit information regarding a suspected or known cyber threat through the applicable SORN, this PIA and related US-CERT 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?

The US-CERT Oversight and Compliance Officer ensures adequate guidelines and procedures are in place and that all US-CERT personnel working in support of the JCSP are familiar with, understand and adhere to those guidelines. The US-CERT Oversight and Compliance Officer conducts quarterly internal reviews to evaluate the program and assess its compliance with applicable guidelines, procedures, and applicable laws and regulations.

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

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 ISSO. 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 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 JCSP training specifically for analysts supporting on the pilot.

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[8] prior to acquiring access to all DHS systems. All users supporting the JCSP have a valid requirement to access the systems and only the type of access required to meet their professional responsibilities. Access is based

[8] 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.

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 Network Manager and ISSO. Accounts are reviewed monthly by the ISSO to ensure that accounts are maintained current. In addition, user account activity is logged, and the logs reviewed each day.

US-CERT also maintains SOPs which describe the necessary procedures to protect PII, defines the terms and outlines roles and responsibilities. SOPs are provided to all US-CERT employees during training.

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 (MOAs) developed between DHS, DoD, the CSPs, and other federal departments and agencies are based on an approved template that has been fully 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 Officials

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

Approval Signature

[Original signed copy on file with the DHS Privacy Office]

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security