Privacy Impact Assessment
for the

National Cybersecurity Protection System (NCPS) - Intrusion Detection

DHS/CISA/PIA-033

September 25, 2019

Contact Point
Martin Gross
Cybersecurity Division
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
(703) 235-2853

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

Abstract

The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Division (CSD) leads the Federal Government effort to protect and defend federal civilian Executive Branch agency networks from cyber threats. These efforts are conducted, in part, through the National Cybersecurity Protection System's (NCPS) intrusion detection capabilities — formerly referred to as EINSTEIN 1 and EINSTEIN 2. This Privacy Impact Assessment (PIA) provides a programmatic update on the NCPS intrusion detection capabilities and provides an in-depth analysis of the collection of information related to known or suspected cyber threats that could potentially include information that could be considered personally identifiable information (PII). Due to the close operational relationship between the NCPS network flow (netflow) and intrusion detection capabilities, this PIA combines, updates, and replaces the former EINSTEIN PIA (September 2004) and EINSTEIN 2 PIA (May 2008).

Overview

The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Division (CSD) designs, develops, maintains, and operates the NCPS. The NCPS is an integrated system that delivers a range of capabilities, including intrusion detection, analytics, intrusion prevention, and information sharing capabilities that are used to defend the Federal civilian Government's information technology infrastructure (hereafter referred to as "federal networks") from cyber threats.[1] This PIA covers the NCPS intrusion detection capabilities and provides an in-depth analysis of the collection of information related to known or suspected cyber threats that could potentially include information that could be considered personally identifiable information (PII).[2] Information on NCPS intrusion prevention capabilities can be found in the EINSTEIN 3 Accelerated PIA.[3] Information on additional NCPS capabilities can be found in the NCPS PIA.[4]

---

[1] The Cybersecurity Information Sharing Act of 2015 defines a cybersecurity threat as an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system (Exclusion: The term "cybersecurity threat" does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement). *See* The Cybersecurity Information Sharing Act of 2015, *available at* https://www.congress.gov/114/bills/s754/BILLS-114s754es.pdf.

[2] DHS Privacy Policy and Compliance Instruction 047-01-001 defines PII as information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual regardless of whether the individual is a U.S. Citizen, lawful permanent resident, visitor to the United States, or employee or contractor to the Department. *See* The DHS Privacy Policy and Compliance Instruction 047-01-001, *available at* https://www.dhs.gov/publication/privacy-policy-and-compliance-instruction-047-01-001.

[3] *See* The EINSTEIN 3 Accelerated (E^3A) PIA, *available at* www.dhs.gov/privacy.

[4] *See* The National Cybersecurity Protection System (NCPS) PIA, *available at* www.dhs.gov/privacy.

NCPS intrusion detection capabilities alert[5] CSD cybersecurity analysts to the presence of malicious or potentially harmful computer network activity in federal network traffic. NCPS intrusion detection capabilities include the passive observation of network traffic travelling to and from participating federal executive agencies' networks as well as an intrusion detection system (IDS) capability that alerts when a pre-defined specific cyber threat is detected.

Network Flow (Netflow) and Metadata Data Collection

The NCPS intrusion detection capability includes an automated process for collecting computer network security information related to traffic to and from federal civilian Executive Branch departments and agencies. This capability works by collecting netflow records.[6] Netflow is a network traffic summarization format widely used by network engineers and security analysts. It summarizes communications between two hosts communicating over the Internet. The collection of netflow records takes place at the agency level and allows federal departments and agencies to monitor their own network activity. Recently enhanced capabilities provide the ability to collect additional packet metadata, such as communication protocols and other attributes. CISA's Netflow collection differs from traditional intrusion detection collection in that select metadata is collected and retained for 90 days, even when not related to a suspected or confirmed cybersecurity threat, to allow CISA cybersecurity analysts the ability to query the data based on known threats.

To date, the data collected from netflow records and packet inspections include the following:

- Autonomous System Numbers (ASN)[7]
- Internet Control Message Protocol (ICMP) Type/Code[8]
- Packet Length[9]
- Sensor identification and connection status[10]

[5] An alert, in the context of NCPS intrusion detection capabilities, is when the system alerts a human analyst to suspected malicious activity.
[6] "Flow records" are records of connections (source IP address, destination IP address, time, port used, and sent to) made to a federal executive agency's IT systems.
[7] An autonomous system is a group of Internet Protocol (IP) networks that adhere to a single routing policy. An Autonomous System Number (ASN) identifies the autonomous system -- networks using the same, specified routing policy -- and enables the autonomous system to exchange information with other autonomous systems.
[8] ICMP is used to communicate control messages on the Internet between hosts/routers.
[9] A packet is specially formatted group of bits containing data, IP address, and control information that is transmitted over a network as a collective unit.
[10] Sensor identification is the description of where the sensor is located so it is clear which network/system/agency the data is coming from. Connection status is simply whether or not the system is receiving information

- Source and destination IP address[11]
- Communication protocols[12]
- Source and Destination port[13]
- TCP Flag information[14]
- Timestamp and duration information[15]

To better correlate known information about malware and cyber threat actors, CSD is expanding the collection of netflow data and metadata fields to include application layer protocol information. This type of protocol information does not include the body of an email message or the payload of a web search, but rather includes the accompanying information that provides the capability for machines to exchange data. Collected application layer protocols may include the following metadata fields:

- Uniform Resource Locators (URL) in HTTP requests: URL information could include organization name, computer name, file names. Examples of URLs are below:
  - ftp://user:apassword@ftp.example.com/file-to-download.adfdf%2009u09a----.txt
  - https://www.example.us/index.php
  - http://dhs.gov
- User Agent[16] Strings: User Agent Strings is the data element that the user agent sends to identify itself in an HTTP request. This information is shared or exposed at the organizational level, and not at the end user level. Examples of User Agent Strings are below:
  - CERN-LineMode/2.15 libwww/2.17b3
  - Googlebot-News
  - Mozilla/5.0 (Android; Mobile; rv:30.0) Gecko/30.0 Firefox/30.0

[11] IP addresses are four octet (32-bit) source or destination addresses that uniquely identify computers either on a given network or on the Internet. Source identifies the device sending the packet; destination identifies the intended recipient.
[12] A protocol is a standardized means of communication among machines across a network.
[13] In the networking world, the term 'port' is a number that identifies the beginning or endpoint of a logical connection. This number is part of the URL (Internet address) right after the domain name.
[14] Simply stated, a TCP flag is a piece of information that is added to packets traveling between computers that describes the status of the connection between the computers. These 'flags' are very specific information, and any abnormality in the way they appear or are paired could be indicative of malicious activity.
[15] A time that is printed to a file (such as email) or other location to help keep track of when data is added, removed, sent, received, etc.
[16] A user agent is software that is acting on behalf of a user. Most commonly, this term refers to a user's Internet browser.

- awi v3. 10.683

- Server Self-Identification Strings: Server Strings could include information such as the host name, domain name, and IP address. Examples of server strings are below:
  - HTTP Server Strings:
    - CERN/3.0 libwww/2.17
    - BaseHTTP/0.2
    - Apache
  - Email Server Strings:
    - Mta1.example.com
    - [192.168.1.1]
    - abuse@example.com
  - SSH[17] Server Strings:
    - SSH-2.0-billsSSH_3.6.3q3
    - OpenSSH_4.3

- Email Headers and Email Transaction Information (i.e., SMTP headers): Email header information could include from, to, date, sender, cc, sender/receiver user ID or email address, email subject,[18] IP address, and domain name, which could include information that could be considered PII.[19] Example of email header data that could be collected:

```
Received: from winhost.example.com (Host-10-11-210-165.example.com
[10.11.210.165] (may be forged))

by {myserver} (8.14.5/8.14.5) with ESMTP id {id}

for {myspamtrap}; Fri, 10 Oct 2014 15:49:53 -0400 (EDT)

Message-Id: <201410101949.{id}@{myserver}>

Received: from User ([10.11.20.214]) by winhost.example.com with
MailEnable ESMTP; Fri, 10 Oct 2014 02:27:18 +0300
```

[17] Secure Shell (SSH) protocol uses encryption to secure the connection between a client and a server. All user authentication, commands, output, and file transfers are encrypted to protect against attacks.
[18] Analysts do not actively monitor email subject lines or any email content, but query such information during the retention period to identify unusual trends based on known or suspected cyber threats. One example of this may be a spear phishing campaign that uses a common subject line that entices an email recipient to open the email, such as offering free tickets to a sporting event. This information is then used to block or triage potentially malicious emails from reaching its anticipated recipient(s).
[19] This information does not include email attachments or the body of the email. However, if an analyst uses the header to determine there is malicious cyber activity, the analyst could then retrieve the full email if collected by the IDS or request the full email from the participating Department or Agency.

```
Reply-To: <example@gmail.com>
From: "Mrs Williams"<postmaster@winhost.example.com>
Subject: Test
Date: Thu, 9 Oct 2014 16:29:14 -0700
MIME-Version: 1.0
Content-Type: text/plain; charset="Windows-1251"
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000
```

- Domain Name System (DNS)[20] Query/Response Data: A DNS query (also known as a DNS request) is a demand for information sent from a user's computer (DNS client) to a DNS server. In most cases a DNS request is sent, to ask for the IP address associated with a domain name. An attempt to reach a domain is actually a DNS client querying the DNS servers to get the IP address related to that domain.
- Secure Sockets Layer (SSL)/Transport Layer Security (TLS)[21] Certificates: SSL/TSL certificate information could include the "common name" (i.e., name of website being identified), the organization running the site, the certificate issuer, when the certificate is valid, and the unique fingerprint of the certificate.

Using the data collected from netflow records, along with the enhanced collected netflow data, CSD cybersecurity analysts can assess and detect certain types of cyber threats (e.g., compromised systems or hosts) and coordinate with the appropriate federal executive departments and agencies to mitigate potential threats and vulnerabilities on their networks. For example, CSD cybersecurity analysts using analytic tools can detect malware communicating over the network, exfiltration of data from federal networks, distributed and non-distributed denial of service attacks, anomalous network activity, and configuration management issues in netflow data.

The ability to correlate similar data across disparate detection methods can only be performed if data is accurately matched and has equivalent meanings between data fields that are acquired using different methodologies. The expansion of the collection of additional netflow data fields will generate strong links between cyber threats observed on the network layer and those

[20] The domain name system, or DNS, is a naming database in which Internet domain names are located and translated into IP addresses. The domain name system maps the name people use to locate a website to the IP address that a computer uses to locate a website.
[21] Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are standard security technologies for keeping an Internet connection secure and safeguarding any data being sent between two machines.

observed at the endpoints. Suspicious traffic can then be validated against known cyber threats identified by CSD cybersecurity analysts or external sources such as other government cybersecurity centers, the private sector, and commercial data sources.

While the data collected via the netflow capability may collect information that includes PII, the data is being collected only for the purpose of addressing a known or suspected cyber threat and is only accessible by CSD cybersecurity analysts when there is an indication of malicious cyber activity that involves that particular dataset. The goal of the collection of this data is to identify cyber threats and protect federal networks, not to collect PII or to identify a specific individual or individuals.

Intrusion Detection System (IDS)

In addition to passively observing network traffic to and from federal networks, the NCPS includes an intrusion detection system (IDS) that generates alerts when specific malicious network activity is detected. The IDS provides CSD cybersecurity analysts with increased insight into the nature of that activity. Using the alert data from the IDS, CSD cybersecurity analysts are able to analyze malicious activity occurring across federal networks resulting in improved situational awareness. This information can then be shared with federal departments and agencies in an effort to mitigate potential cyber threats and vulnerabilities on their networks.

The IDS employs "signature-based intrusion detection" to detect potentially malicious traffic travelling to and from federal networks. This intrusion detection method compares network traffic to a set of pre-defined signatures,[22] and triggers an alert when a match is detected. CSD cybersecurity analysts are alerted when a known signature or suspected threat is observed by the IDS sensors, at which point the information is analyzed and shared with appropriate partners, then a response, mitigation, and recovery can be coordinated, if necessary.

The IDS is not programmed to specifically collect or locate PII. Signatures might be developed in response to known or suspected cyber threats using indicators[23] containing information that could be considered PII (such as an email address); however, the purpose of the signatures is to identify the cyber threats, not to identify or collect PII. Accordingly, while the IDS could collect information that includes PII, the collected information would be directly related to a cyber threat being transmitted to or from federal civilian Executive Branch agency networks. The goal of the IDS is to identify the cyber threat and protect federal networks, not to collect PII or to identify a specific individual or individuals. For example, if a security exploit chose to use

[22] Signatures are derived from numerous sources and are specific machine-readable patterns of network traffic that affect the integrity, confidentiality, or availability of computer networks, systems, and information. For example, a specific signature might identify a known computer virus that is designed to delete files from a computer without authorization.

[23] 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 IP addresses, domains, email headers, files, and strings.

an email address or other information that could be considered PII in the delivery of malicious code, a signature could be deployed via the IDS in response to that exploit that could contain that information.

Signature Review Process

Signatures deployed within the IDS must adhere to applicable CSD information handling guidelines, standard operating procedures (SOP), and policies. Periodic reviews are conducted by CSD leadership, the Office of the Chief Counsel, and the CISA Office of Privacy. Specifically, the CISA Office of Privacy periodically reviews a statistically significant sample of IDS signatures that were deployed by CSD cybersecurity analysts during the reporting period.

These reviews ensure that IDS signatures are:

- Not overly broad in scope;
- Not inappropriately targeting PII;
- Based upon a known or suspected cybersecurity risk;
- Deployed in a manner that directly supports CSD's cybersecurity and network defense mission; and
- Created and deployed as is reasonably necessary to protect agency information and agency information systems from a cybersecurity risk.

Since 2012, following recommendations from the DHS Privacy Office's EINSTEIN Privacy Compliance Review (PCR),[24] the CISA Office of Privacy has carried out the Privacy Oversight Review for PII Handling on a biannual basis. As noted in the DHS Privacy Office's 2014 EINSTEIN PCR Update,[25] reviews "provide consistent and regular opportunities to verify that PII is being handled appropriately, and assist in refining procedures to implement the most effective privacy protections for the EINSTEIN program."

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 following authorities that permit and define the suite of NCPS capabilities include the following:

- *Homeland Security Act of 2002, as amended by the Cybersecurity Act of 2015* and the Cybersecurity and Infrastructure Security Agency Act of 2018, requires that DHS

[24] *See* DHS Privacy Compliance Review for the EINSTEIN Program, *available at* https://www.dhs.gov/publication/privacy-compliance-review-einstein-program.
[25] *See* The Privacy Compliance Review Follow-Up Letter (August 26, 2014), *available at* https://www.dhs.gov/sites/default/files/publications/einstein%20pcr%20ltr%20august%202014.pdf.

deploy, operate, and maintain intrusion detection and prevention capabilities to be employed by federal departments and agencies. Section 223(b) of the Federal Cybersecurity Enhancement Act of 2015 requires agencies to use these intrusion detection and prevention capabilities. Agencies also execute a memorandum of agreement (MOA) with DHS relating to the deployment of EINSTEIN capabilities.

- *Homeland Security Act of 2002, as amended by the National Cybersecurity Protection Act of 2014*, establishes and authorizes various functions for the National Cybersecurity and Communications Integration Center, including its role as a federal civilian interface for sharing information related to cybersecurity risks and incidents.

- *Subchapter II of chapter 35 of title 44, U.S. Code, as amended by the Federal Information Security Modernization Act of 2014 and subsequent statutes,* establishes authorities of the Office of Management and Budget, DHS, and all federal Executive Branch civilian agencies in securing federal information systems. It also establishes a federal information incident security center within DHS.

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

Information regarding known or suspected cyber threats that is collected through the NCPS intrusion detection capabilities is not based on data that identifies an individual, but rather on the security event that triggered an alert. In the rare cases where the NCPS intrusion detection capabilities collect PII, this information will be maintained and indexed by the security incident, and not by a personal identifier. Therefore, the Privacy Act does not apply to NCPS intrusion detection records and a SORN is not required.

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

The core components of NCPS (FISMA # PRE-00380-GSS-00380), which includes the intrusion detection capabilities, received an Authority to Operate (ATO) on July 13, 2016.

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

DHS retains information obtained through the NCPS only to protect information and information systems from cybersecurity risks. DHS retains information obtained through the NCPS no longer than is reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk. A records retention schedule for NCPS

(Record Schedule #DAA-0563-2013-0008) was approved on January 12, 2015.[26] NCPS intrusion detection data is destroyed or deleted when three years old or when no longer needed for agency business, whichever is later. PII that is determined not to be directly related to known or suspected cyber threats or vulnerabilities will be deleted immediately.

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 to the information collected by the NCPS intrusion detection capabilities.

Section 2.0 Characterization of the Information

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

NCPS intrusion detection capabilities collect information regarding known or suspected cyber threats from network traffic transiting to and from federal networks. The information collected takes the form of netflow records and network packets collected in response to alerts triggered by pre-determined intrusion detection signatures. When a signature for a known or suspected cyber threat triggers an alert, that data is captured along with a predetermined amount of associated traffic that is analytically relevant to that particular threat. This additional data could include IP addresses, ports, protocols, digital signatures, time stamps, direction/type of traffic, flags, sensor name, etc.

CSD uses analytically relevant data to develop indicators of malicious cyber activity, which are then used to create and deploy intrusion detection signatures into the IDS to detect and mitigate cyber threats. An indicator can be identified as human-readable cyber data used to identify some form of malicious cyber activity and can be related to IP addresses, domains, email headers, files, and strings.

Information collected from NCPS intrusion detection capabilities will also be used to detect and correlate anomalies across agency networks. These anomalies include, but are not limited to,

[26] *See* The NARA Records Schedule, DAA-0563-2013-0008, *available at* http://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/daa-0563-2013-0008_sf115.pdf

configuration problems, unauthorized network traffic, network backdoors, routing anomalies, network scanning activities, and baseline network patterns.

As part of its computer network security responsibilities, CSD may use the resulting analysis of information collected by NCPS intrusion detection capabilities to generate reports on topics including general computer network security trends, specific incidents, and anomalous or suspicious activity observed on federal networks. The identification of the specific individual that established the network connection that triggered an alert is not included in the reports. These reports are made available to DHS organizations, and other federal executive agencies through systems such as the US-CERT.gov secure website for their use in infrastructure protection and other computer network security related responsibilities. CSD shares analysis, along with additional computer network security products, with its partners and stakeholders (federal departments and agencies, state, local, and tribal governments, industry, academia, the general public, and international partners) via its website: www.us-cert.gov.

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

As mentioned in Section 2.1, the source of the information includes the IDS sensors themselves, which are located at various federal agency network collection points. The sensors push netflow records to the data store on a consistent basis and do not require analyst intervention.

For the development of intrusion detection signatures, cyber threat information is received by CSD from a number of sources including the following: analysis by CSD's cybersecurity operations teams, data submitted to CSD from other government departments and agencies, reports received from mission and industry partners, and commercially available cyber threat data services.

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

CSD cybersecurity analysts use information from a range of sources, including commercial sources and publicly available data related to cybersecurity threats (e.g., anything that could be found through open source Internet searches, newspaper articles). This data is used to understand cyber events that are reported to CSD and for historical reference of similar incidents. CSD only uses commercial or publicly available data that is relevant to the CISA cybersecurity mission of protecting federal networks and does not use it for the purpose of identifying individuals.

2.4 Discuss how accuracy of the data is ensured.

NCPS intrusion detection capabilities are not designed to manipulate or modify any data. Rather, the intrusion detection hardware maintains exact copies of the information specified above, as transmitted to or from federal networks. For example, if a connection "spoofs" an IP address (manipulates the data packets it transmits to a federal network to appear as if being sent from one source when in fact they come from another source) the intrusion detection system will simply record those packets with the "spoofed" IP address. The system only keeps a copy of the spoofed IP address; therefore, data collected by a sensor is accurate because it is an exact copy of the data available.

In addition, signatures are reviewed and approved by CSD in accordance with its written procedures and information handling guidelines. These procedures include validating the signatures to ensure they are active, useful, and within policy guidelines before being deployed. CSD also continuously monitors the production environment to verify expected results.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that NCPS intrusion detection capabilities may collect PII from network traffic that is not necessary to understand or analyze a cyber threat.

Mitigation: The risk is mitigated. Network traffic data collected by NCPS intrusion detection capabilities may only be accessed by CSD cybersecurity analysts and only in cases where the traffic is related to a known or suspected cybersecurity threat. If network traffic does not meet the criteria to trigger an IDS alert or analyst query, then that network traffic is not viewed by CSD cybersecurity analysts.

Additionally, all data that could potentially contain PII is managed in accordance with the appropriate CSD SOPs and information handling guidelines. Specifically, all potential PII is reviewed prior to being included in any analytical products or other forms of dissemination. CSD information handling guidelines require that PII be removed or replaced with a generic label whenever it is not necessary to analyze or understand a cyber threat. In some cases, a product may include PII because that information is deemed analytically relevant and necessary to understanding the cyber threat. In those instances, CSD SOPs and information handling guidelines provide safeguards for the marking, dissemination, and handling of the information. Additionally, CSD conducts periodic oversight reviews on IDS signatures to ensure that applicable SOPs and information handling guidelines are being followed.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

Netflow records, signatures, alerts, and portions of network traffic containing malicious activity are used to identify and respond to network security incidents and anomalies, generate reports for distribution to agencies that employ NCPS intrusion detection capabilities and other partners, and increase the resiliency of Federal Government networks.

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.

NCPS intrusion detection capabilities provide query and analytical capabilities of collected data to fulfill the mission requirement. The IDS retrieves information by the security event that triggered an alert, not by information related to an individual. Applicable SOPs and information handling guidelines require that query and search criteria be based on a characteristic of a known or suspected cyber threat or incident. In addition, queries and searches must be conducted for the purpose of protecting federal networks or detecting, analyzing, mitigating, and preventing known or suspected cyber threats or incidents.

CSD cybersecurity analysts will review the results of queries and searches to determine if PII is present. Reviews are conducted regardless of the source of the information, even if it appears that the information has been collected in accordance with applicable laws and policy. If it is determined that PII is present, then applicable CSD SOPs and information handling guidelines require that CSD cybersecurity analysts determine whether that information is necessary to understand or analyze a cyber threat. PII that is deemed not to be directly related to a cyber threat will be purged and omitted from analysis and other CSD products.

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

No. Only CSD cybersecurity analysts and NCPS system administrators have access to the components of the NCPS system used for analysis and reporting. All NCPS capabilities and systems are governed by principles of least privilege, which limits user privileges for viewing and processing data within NCPS capabilities and systems.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk that PII inadvertently obtained via NCPS intrusion detection capabilities will be used inappropriately.

Mitigation: This risk is mitigated. CSD cybersecurity analysts, as well as NCPS system administrators and information assurance personnel, are trained on both DHS and CSD specific procedures for handling and safeguarding PII. Those personnel receive training upon being hired and are also required to complete annual refresher training. In addition, CSD maintains SOPs and guidelines for the identification of sensitive information, the proper handling and minimization of PII, and to define the terms of use for specifically identified roles and responsibilities.

Access to the NCPS and its intrusion detection capabilities is restricted to government and contractor staff with a demonstrated need for access, and such access requires approval by a supervisor and NCPS system managers and account management personnel. Authorized users[27] must sign Rules of Behavior that identifies the need to protect PII prior to gaining access to the NCPS and strict disciplinary measures are in place for violations of those rules. NCPS user actions are logged and users are informed in advance of that condition prior to account issuance.

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.

Users of federal computer systems are provided with log-on banners and/or are required to sign user agreements that specifically notify them of and obtain consent for computer network monitoring, appropriate uses of the system, and unauthorized uses of the system. Furthermore, 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 is monitored. Such notices cover NCPS intrusion detection capabilities.

Agencies that employ NCPS intrusion detection capabilities are required to certify to CSD that they have appropriate notices, banners, or other measures in place to provide individuals with notice that their interaction with federal networks is subject to monitoring for computer network security purposes.

Sample notice language for log-on banners, user agreements, and privacy policies is provided to federal civilian departments and agencies as part of the MOA with CSD. These are provided for reference in Appendices A, B, and C of this PIA.

This PIA and previously published DHS cybersecurity-related PIAs also serve as general notice to individuals that network traffic flowing to or from federal civilian departments and agencies may be collected for network security purposes.

[27] The term "authorized users" in this document refers to authorized and trained federal employees, contractors, and other individuals that have been granted access to the NCPS and its related components.

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

All users logging into a federal agency network that employs NCPS intrusion detection capabilities are presented with an electronic notice or banner that notifies them that government computer systems are monitored. Notice may also be provided as part of those agencies' public-facing website privacy policies and through links from those policies, via the DHS Cybersecurity and Privacy webpage.[28] Those privacy policies state that the agency uses computer security programs to monitor network traffic. Users inside the agency network receive notice by their agency's use of log-on banners and/or 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.

Once an individual decides to communicate with an agency electronically, the network traffic is subject to network security efforts of CSD, including NCPS intrusion detection capabilities, in addition to any specific computer security programs the agency might have in place.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that a person may not be aware of or understand that network traffic may be collected under NCPS intrusion detection capabilities.

Mitigation: This risk is mitigated. DHS provides a variety of notice mechanisms to users (both internal and external) of federal systems and networks. The participating agency's website privacy policy states that the agency uses computer security programs to monitor network traffic. Users inside the agency networks receive notice by the agency's use of log-on 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 NCPS-related PIAs or visit the DHS Privacy website that provides additional resources explaining the DHS cybersecurity mission and programs.[29]

Section 5.0 Data Retention by the project

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

DHS will retain information obtained through NCPS intrusion detection capabilities only to protect information and information systems from cybersecurity risks. Data collected through NCPS intrusion detection capabilities is retained in accordance with the approved records retention

[28] *See* The DHS Cybersecurity and Privacy webpage, *available at* https://www.dhs.gov/cybersecurity-and-privacy.
[29] *See* The DHS Privacy webpage, *available at* www.dhs.gov/privacy.

schedule for the NCPS (DAA-0563-2013-0008). Intrusion detection data is retained for three years or until it is no longer needed for agency business, whichever is later.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that PII may be inadvertently collected and retained beyond what is necessary to appropriately analyze or address a cybersecurity threat.

Mitigation: This risk is mitigated. CSD cybersecurity analysts determine if any and all PII encountered is necessary to analyze or understand the cybersecurity threat. CSD information handling guidelines and SOPs provide the procedures for the collection processing, retention, and dissemination of PII. If PII is determined to not be necessary to analyzing or understanding a threat, it is deleted immediately.

In addition, CSD has worked with NARA to develop an approved records retention schedule for NCPS records (DAA-0563-2013-0008), which states that intrusion detection data will be retained for three years or until it is no longer needed for agency business, whichever is later.

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.

Federal departments and agencies have access to their netflow records and receive information about their own data specific to their networks in accordance with CSD's applicable SOPs and information handling guidelines. CSD cybersecurity analysts may also share the raw network information pursuant to individual signatures with the specific agency on whose network the malicious activity was discovered. This allows for further analysis of the activity. Additionally, information collected, analyzed, or otherwise obtained by CSD in connection with known or suspected cybersecurity threats or incidents may be disclosed as part of work products.

CSD shares analysis along with additional computer network security products with its partners and stakeholders (federal departments and agencies; state, local, and tribal governments; academia, industry, and international partners; and the general public) via the US-CERT.gov website, the Homeland Security Information Network (HSIN),[30] and, on a case-by-case basis, directly.

[30] The HSIN portal provides a secure, web-based, and interactive system to allow collaboration among CSD team members, constituents, partners, and stakeholders so that they may share timely, accurate, and actionable cybersecurity information with one another in a trusted and secure environment. The HSIN portal institutionalizes trusted environments among clearly defined user groups within its user community by providing secure compartments for distinct cybersecurity coordination.

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

Information collected by NCPS intrusion detection capabilities is not based on data that identifies an individual, but rather on the security event that triggered the alert. 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 records by a personal identifier does the Privacy Act require a SORN. Because CSD does not retrieve NCPS intrusion detection information by a personal identifier, a SORN is not required.

6.3 Does the project place limitations on re-dissemination?

CSD generates cybersecurity reports on general cybersecurity trends, cybersecurity incidents, and anomalous or suspicious activity observed on federal networks. These reports, as well as secure messages, forums, and other collaboration tools, are available to organizations within the Department, federal agencies, and other cybersecurity partners via the US-CERT.gov website and HSIN. Some of the information disseminated to these partners may contain or be derived from NCPS intrusion detection data.

Cyber threat information received through NCPS intrusion detection capabilities is reviewed to determine if it contains PII and if so, that information is reviewed and only disseminated if sharing the actual information is analytically relevant to the cyber threat. If PII needs to be disseminated to external stakeholders, written approval must be obtained from CSD leadership in advance of dissemination, in accordance with the appropriate CSD SOPs and information handling guidelines.

Dissemination and re-dissemination are governed by the Traffic Light Protocol, or TLP. TLP was created in order to facilitate greater sharing of information. It is a set of designations used to ensure that sensitive information is shared only with the appropriate audience. TLP employs four colors to indicate expected sharing boundaries to be applied by the recipient(s) of a product of dataset. If a recipient needs to share information more widely than indicated by the original TLP designation, they must obtain explicit permission from the original source.

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

CSD provides cyber-related information to the public, federal departments and agencies, and state, local, tribal and international entities through a variety of products, many of which are available on the US-CERT.gov website.

No formal reports disseminated via the US-CERT.gov website contain PII. Each report is numbered and catalogued, and references exist in all products to tie back to a single incident or series of incidents that precipitated the product itself. In the event that PII must be released, it is released in accordance with the Privacy Act of 1974, appropriate CSD SOPs, and information handling guidelines, and with the authorization and/or written approval of CSD leadership.[31]

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that PII obtained via NCPS intrusion detection capabilities will be shared inappropriately.

Mitigation: The risk is mitigated. Only information that is necessary to understand cyber threats will be included in any of these products. When such authorized dissemination includes information associated with a specific individual, dissemination will comply with the requirements of SOPs and established cybersecurity information handling guidelines.

Appropriate CSD SOPs and information handling guidelines provide instructions for the marking and handling of data for further dissemination. SOPs require that reports that contain PII include markings for the first reference to each instance of the PII. If the report is modified for multiple audiences, each version is reviewed for appropriate markings. Handling and dissemination instructions are also included in the SOPs and information identifying sources and methods from all CSD reports and products are required to be redacted prior to dissemination.

Section 7.0 Redress

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

NCPS intrusion detection information is not based on data that identifies an individual, but on the security event that triggered the alert. In rare cases where NCPS intrusion detection capabilities collect information that could identify a specific individual (e.g., an un-spoofed email address within header information or other PII within records incidentally collected as part of a security incident), this information will be maintained and indexed by the security incident, not by the PII. This means that there will not be a list of email addresses or names maintained, but rather a log of what intrusion or security event occurred; analysts will sort the data by pulling up security events, not by email addresses.

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

[31] 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 with whom it is associated.

Information Act (FOIA) or Privacy Act (PA) request to the DHS/CISA FOIA Officer. Individuals may obtain instructions on how to submit a FOIA/PA request at https://www.dhs.gov/how-submit-foia-or-privacy-act-request-department-homeland-security.

The release of information is subject to standard FOIA exemptions and, given the nature of the cyber threat information contained in the NCPS, CSD may not always disclose to a requester or grant a request for amendment of their record(s). Records, as defined by the Privacy Act, would only consist of log-in/contact information covered under the GITAARS SORN.

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 information collected by NCPS intrusion detection capabilities because flow records and alerts are generated from exact copies of network traffic and are not based on information that identifies individuals.

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 FOIA or PA request to the DHS/CISA FOIA Officer. Individuals may obtain instructions on how to submit a FOIA/PA request at https://www.dhs.gov/how-submit-foia-or-privacy-act-request-department-homeland-security.

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

This PIA, along with other NCPS-related PIAs, serve as notification to the public of proper avenues in place for the public to contact the Department regarding information collections, including procedures for accessing and correcting 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 FOIA or PA request to the DHS/CISA FOIA Officer. Individuals may obtain instructions on how to submit a FOIA/PA request at https://www.dhs.gov/how-submit-foia-or-privacy-act-request-department-homeland-security.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will want to seek redress procedures for PII associated with a known or suspected cyber threat, but are unable to.

Mitigation: This risk is partially mitigated. There are no additional redress procedures beyond those described in Sections 7.0, 7.1, and 7.2 above because information collected through NCPS intrusion detection capabilities is not based on data that identifies an individual but instead on the security event that triggered the alert. Information is retrieved, stored, and reported by the

security event that triggered the alert. As such, there is no information about an individual that can be used to access the cybersecurity threat or event(s).

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?

CSD has developed SOPs and information handling guidelines that govern the collection, handling, and dissemination of cybersecurity information. The Compliance and Oversight Officer provides guidance and oversight to ensure that cybersecurity information is handled in accordance with those SOPs and guidelines. In addition, the CISA Office of Privacy performs bi-annual privacy oversight reviews to ensure that there is no unnecessary collection or dissemination of PII associated with CSD's intrusion detection capabilities.

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

All DHS employees are required to complete annual Privacy Awareness Training. In addition, CSD cybersecurity analysts are required to participate in periodic training on the procedures and guidelines for the handling of cybersecurity information. This training includes instructions on how to manage privacy risk when developing and deploying new signatures, analyzing netflow records, creating reports, and sharing incident information with partners.

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[32] prior to acquiring access to NCPS systems. All NCPS users must have a valid need to access the system and receive only the type of access required to meet their specific job duties and responsibilities. Access is based upon the role identified on the user's access request form (i.e., analyst, user, general user, system administrator, network administrator). System roles are pre-defined and approved by functional managers within CISA. A user requiring an exception to the standard role for his or her organization must get approval from the functional area within CISA. The NCPS access request form must be completed either by the user for account updates or by current NCPS user for new accounts. The functional area managers validate the need to know in the approval process.

[32] The suitability determination is a process that evaluates 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.

Additionally, users are required to sign a Rules of Behavior document prior to gaining access to the system and complete security awareness training. This training is required annually. Per DHS 4300A policy,[33] accounts are subject to disablement for non-compliance. User accounts are disabled after 30 days of inactivity or promptly upon departure from the organization.

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 MOAs between DHS and other federal civilian government departments and agencies are based on an approved template that has been coordinated and approved by the program manager, system owner, Office of General Counsel, and the CISA Office of Privacy. Agreements are reviewed periodically and updated when data usage, privacy policies, access procedures, or other conditions are identified. New uses of the information and new access to the system by organizations within DHS and outside are similarly reviewed by various stakeholders, including integrated program teams with approval vetted through upper management.

Responsible Officials

Jeanette Manfra
Assistant Director
Cybersecurity Division
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office

_____

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

[33] DHS 4300 is a series of information security policies, which are the official documents that create and publish Departmental security standards in accordance with DHS Management Directive 140-01 *Information Technology System Security*.

Appendix A: Sample Language for Log-on Banner for Federal Networks

- You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.
- Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.
- By using this information system, you understand and consent to the following:
  - You have no reasonable expectation of privacy regarding any communications or information transiting, stored on, or traveling to or from this information system. At any time, the government may for any lawful government purpose monitor, intercept, search, and seize any communication or information transiting, stored on, or traveling to or from this information system.
  - Any communications or information transiting, stored on, or traveling to or from this information system may be disclosed or used for any lawful government purpose.

[click button: "I AGREE"]

NOTE: For purposes of such banners, agencies shall ensure that references to monitoring by the government are sufficient to address activities undertaken by government contractors.

Appendix B: Sample Language for Department and Agency User Agreements

By signing this document, you understand and consent to the following when you access this agency's information systems, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices (e.g., BlackBerry, PDA) and storage media (e.g., thumb drive, flash drive) attached to this network or to a computer on this network:

- You are accessing a U.S. Government information system that is provided for U.S. Government-authorized use only;
- Unauthorized or improper use of the information system may result in disciplinary action, as well as civil and criminal penalties;
- The Government, acting directly or through its contractors, routinely monitors communications occurring on this information system. You have no reasonable expectation of privacy regarding any communications or data transiting, stored on, or traveling to or from this information system. At any time, the government may for any lawful government purpose monitor, intercept, search, and seize any communication or data transiting, stored, or traveling to or from this information system;
- Any communications or data transiting, stored on, or traveling to or from this information system may be disclosed or used for any lawful government purpose.

I understand and consent.

<<SIGNATURE BLOCK TO BE INSERTED LATER>>

Appendix C: Sample Language for Privacy Policy

<<AGENCY NAME>> information systems may be protected by EINSTEIN cybersecurity capabilities, under the operational control of the U.S. Department of Homeland Security's Cybersecurity Information Security Agency (CISA). Electronic communications with <<AGENCY NAME>> may be scanned by government-owned or contractor equipment to look for network traffic indicating known or suspected malicious cyber activity, including malicious content or communications. Electronic communications within <<AGENCY NAME>> will be collected or retained by CISA only if they are associated with known or suspected cyber threats. CISA will use the information collected through EINSTEIN to analyze the known or suspected cyber threat and help <<AGENCY NAME>> and other agencies respond and better protect their computers and networks.

For additional information about EINSTEIN capabilities, please see the EINSTEIN program-related Privacy Impact Assessments available on the DHS cybersecurity privacy website (https://www.dhs.gov/privacy-documents-national-protection-and-programs-directorate-nppd) along with other information about the Federal Government's cybersecurity activities.