Privacy Impact Assessment

for the

National Cybersecurity Protection System (NCPS) - Core Infrastructure

DHS Reference No. DHS/CISA/PIA-035

August 10, 2020

Homeland Security

Abstract

The U.S. 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 (NCPS). The platforms and systems upon which the NCPS intrusion detection, analytics, intrusion prevention, and information sharing capabilities rely are called the NCPS Core Infrastructure. This Privacy Impact Assessment (PIA) provides an in-depth analysis of the collection of information through the operation of the NCPS Core Infrastructure. CISA is in the process of developing separate PIAs to document the privacy implications for each of the NCPS's capability areas (Intrusion Prevention, Intrusion Detection, Analytics, Core Infrastructure, and Information Sharing). Once published, these PIAs will eventually replace the currently published DHS/CISA/PIA-026 National Cybersecurity Protection System (NCPS).

Overview

The DHS CISA CSD designs, develops, maintains, and operates NCPS, an integrated system that delivers a range of capabilities, including intrusion detection,[1] 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.[2] This PIA covers the NCPS Core Infrastructure, which is comprised of the following platforms, capabilities, tools, and systems:

- Mission Operating Environment (MOE)
- Top Secret Mission Operating Environment (TS MOE)
- NCPS Incident and Event Management
- Development & Test Environment (DTE)
- Development, Security, and Operations (DevSecOps)

[1] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, PRIVACY IMPACT ASSESSMENT FOR THE NATIONAL CYBERSECURITY PROTECTION SYSTEM (NCPS)-INTRUSION DETECTION, DHS/CISA/PIA-033 (2019), *available at* https://www.dhs.gov/privacy-documents-cisa.

[2] Cyber threats can be defined as any identified efforts directed toward accessing, exfiltrating, manipulating, or impairing the integrity, confidentiality, security, or availability of data, an application, or a federal system, without lawful authority. Information about cyber threats may be received from government, public, or private sources. Categories of cyber threats may include, for example: phishing, Internet Protocol (IP) spoofing, botnets, denials of service, distributed denials of service, man-in-the-middle attacks, or the insertion of other types of malware. *See* CYBERSECURITY ACT OF 2015, Pub. L. No. 114–113, Division N, Title I, § 102, 129 Stat. 2936 (2015) (current version at 6 U.S.C. § 1501(5)(a)).

- Learning Management System (LMS)
- External Web/Internet Application Hosting Environment (EWAH)

Mission Operating Environment (MOE)

The MOE is a dedicated network environment upon which NCPS intrusion detection, intrusion prevention, analysis, and information sharing capabilities are hosted. The MOE provides the infrastructure required for the NCPS to accomplish its cybersecurity mission and is the communications network and operating system used exclusively by CISA to conduct daily cybersecurity operations.[3] The MOE is also used as the platform from which NCPS applications issue regular security and warning bulletins and receive public contribution and outreach. The MOE may collect PII, such as contact information from those who contribute security alerts or those who receive warning bulletins.

The MOE also maintains its own Active Directory for email distribution list purposes and to assign permissions to shared resources. The MOE Active Directory includes the following information: name, userID, email address, and organization name. Only general MOE account access information, such as user name/ID and organization name, can be used to retrieve user information. This is done to establish MOE account access, provide password resets, and provide user account-unlock capabilities.

Top Secret Mission Operating Environment (TS MOE)

The NCPS Mission Operating Environments include both unclassified and classified (TS/Special Compartmented Information SCI) components. The TS MOE supports NCPS intrusion prevention capabilities as well as Enhanced Cybersecurity Services.[4] The classified information and tools used for the analysis performed on the TS MOE requires the network to be isolated from all other NCPS and DHS networks. The network has been structured to allow for analysis while protecting itself, as necessary, through the use of firewalls, intrusion detection systems, intrusion prevention systems, encryption, smart switches, and multiple other layers of security.

NCPS Incident and Event Management

The NCPS includes an incident and event management capability to track, control, and manage mission events, service requests, and reported incidents. Individuals from the private and

[3] As the system developer and operator, CISA also uses the MOE to provide user support to CISA cybersecurity analysts and to deploy and maintain NCPS capabilities.
[4] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, PRIVACY IMPACT ASSESSMENT FOR THE ENHANCED CYBERSECURITY SERVICES (ECS), DHS/CISA/PIA-028 (2013 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-cisa.

public sector may contact CISA on a 24/7 basis to report cyber incidents, submit service requests, and provide other related reports that are collected by this capability.

Information is collected via telephone, email, or web form. The individual's contact information (first name, last name, email address, phone number, and organization) and the nature of the concern are collected and documented by CISA personnel. Once recorded, a ticket is created, and notification for handling is sent to the appropriate team within CISA (e.g., malware analysts, NCPS system administrators, and other CISA cybersecurity analyst teams). Contact information and relevant correspondence information is voluntarily collected to coordinate incident response activities, respond to requests, and facilitate customer relationship management activities.

Development and Test Environment (DTE)

The NCPS DTE provides the infrastructure and software tools needed to test new and existing capabilities for deployment in a simulated end-to-end NCPS system prior to deployment to production. This initial DTE deployment allows CISA to mitigate potential vulnerabilities and reduce potential impacts when transitioning to the operational environment.

The DTE allows CISA to execute a unified approach to develop and test cybersecurity services and capabilities. This environment simulates the current NCPS operational systems, connectivity, capabilities, and identifies the development and testing environment configurations needed to meet project requirements. These combined capabilities also allow CISA to accurately define the hardware, software, and human resources needed to meet long-term program requirements.

The DTE also allows CISA cybersecurity analysts to experience and train with new capabilities before they are deployed into the production network. This serves to increase knowledge transfer to better support operations, demonstrate critical performance metrics, such as load, capacity, and user interface, and provides an environment to showcase prototypes and validate emergency repairs.

The DTE uses both synthetic data and operational data for test purposes, which may be stored temporarily within the development and test environment infrastructure. A subset of NCPS operational cybersecurity data may include packets, files, system logs, and netflow records which may include PII.[5] Other subsets of NCPS data include analytically relevant data and can include email addresses, real or spoofed IP addresses, and digital signatures. The DTE only retains data that is necessary to accomplish its development and testing purpose. Specific technical,

[5] This includes Uniform Resource Locators (URL) in HTTP requests, User Agent Strings, Server Self-Identification Strings, Email Headers and Email Transaction Information, Domain Name System (DNS) Query/Response Data, and Secure Sockets Layer (SSL)/Transport Layer Security (TLS) Certificates. For more information about these fields, *see* U.S. DEPARTMENT OF HOMELAND SECURITY, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, PRIVACY IMPACT ASSESSMENT FOR THE NATIONAL CYBERSECURITY PROTECTION SYSTEM (NCPS)-INTRUSION DETECTION, DHS/CISA/PIA-033 (2019), *available at* https://www.dhs.gov/privacy-documents-cisa.

operational, and managerial controls are implemented to ensure a safe and appropriately secure environment necessary to provide functional capabilities for the development and testing of new tools.

The DTE uses approved and standardized data sets determined by the Information System Security Officer (ISSO), which are available to all NCPS development projects. The test environment does not contain sensitive information that merits special handling. New and enhanced capabilities only operate in this non-production environment throughout the development and testing stages of the engineering lifecycle.

Development, Security, and Operations (DevSecOps)

DevSecOps eliminates the fragmented execution of the system development process by consolidating the development, security integration, testing, and operations phases into a single collaborative environment. The DevSecOps capability automates the execution of critical activities currently executed manually in support of the system development lifecycle.

DevSecOps systems are hosted within a commercial provider's cloud environment and are protected at the level approved by the Federal Risk and Authorization Management Program (FedRAMP), a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. In order to ensure the appropriate level of IT security, the cloud provider is subject to FedRAMP high and moderate confidentiality, integrity, and availability baselines which allow customers to host sensitive Controlled Unclassified Information (CUI) and all types of regulated workloads.

Information stored, processed, and transmitted by DevSecOps systems includes the following:

- Scripts that automate the configuration and deployment of multiple servers;
- Functional test results;
- Security scan results;
- Application source code;
- Operating system images;
- System logs; and
- Documents that describe actions taken to resolve functional/security test failures.

Learning Management System (LMS)

The LMS is a technical mentoring system that is supported via the NCPS MOE. It provides the software tools to create, assign, and track learner training, and includes a central repository of training material accessible by mentors and learners. The system is used to author courses and

mentoring videos to train CISA cybersecurity analysts in systems, software, and techniques needed to ensure they are able to detect and respond timely to malicious cyber activity or threats that may be present on federal networks. The LMS is also used to develop and provide role-based training for all MOE user roles (e.g., system administrators, information assurance personnel).

Specifically, the LMS provides:

- Access to a central repository for training materials;
- The ability to assign one or multiple courses to personnel, based on the particular function, role, and level of support they provide;
- Centralized enrollment and approval;
- Restricted access to specific courses;
- Capability for users to evaluate courses; and
- Course usage statistics (e.g., number of students accessing the course, amount of time individual students spent in a course, and specific answers to test questions).

The LMS uses the user name/ID and organization name in the MOE Active Directory to assign training to the appropriate users/roles and to track course access and course completion.

External Web/Internet Application Hosting Environment (EWAH)

EWAH is a secure infrastructure for hosting Web/Internet applications that are supported by the NCPS. This infrastructure/hosting environment provides security scanning, network services, storage, and computing resources. EWAH also provides isolation between the hosted applications, the external web environment, and the MOE, with limited, highly controlled connections. Finally, it provides the infrastructure necessary to support secure external data sharing, secure ingest, data and application access control, data transfer/routing, persistent network transport services, processing, and storage to support the hosting of web applications.

EWAH includes an on-premise component that is attached to the MOE. The capability also includes a cloud instance, provided through a commercial cloud service provider (referred to as CEWAH), which operates as the failover capability for applications hosted in the on-premise instance.

EWAH does not collect or generate information about individuals, however, it may, in some instances, host applications that contain PII. The applications/systems hosted in this environment will each have their own authority to operate, as well as their own necessary privacy compliance documentation, which cover the collection of any information collected, generated, or retained by those applications. EWAH may retain information pertaining to administrators of the environment to authenticate and authorize access to infrastructure components.

Information stored by EWAH includes the following:

- *Event and audit logs:* All infrastructure components will record specified events including source of event, host name, and user, in local logs that will be sent to the NCPS Security Information and Event Management (SIEM) system for aggregation and storage within the infrastructure.
- *Scan and compliance results*: Compliance and vulnerability scanning tools will be employed within the infrastructure.
- *Active Directory database*: The environment queries the MOE Active Directory to facilitate authentication and authorization for administrators of the infrastructure.

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 permit and define the suite of NCPS capabilities:

- *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 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 intrusion detection and prevention capabilities. Agencies also execute a memorandum of agreement (MOA) with DHS relating to the deployment of these capabilities.
- *Homeland Security Act of 2002, as amended by the National Cybersecurity Protection Act of 2014*, establishes and authorizes various functions for CISA's cybersecurity operations, 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?

The DHS system of records notice titled, DHS/ALL-016 Correspondence Records, 83 Fed. Reg. 48645 (September 26, 2018), covers the following collection:

- Cyber threat incident report information to submitted to CISA via telephone, fax, or the Internet, including voluntarily provided contact information.

The DHS system of records titled, DHS/ALL-004 General Information Technology Access Account Records Systems, 74 Fed. Reg. 49882 (September 29, 2009), covers the following collection:

- General contact and other related information maintained on the MOE Active Directory used to grant access to employees and contractors to the MOE and TS MOE and compartments within the portal.

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

The DTE received its Authority to Operate (ATO) on March 7, 2018. The TS MOE received its ATO on August 31, 2016. DevSecOps and CEWAH are currently in the process of obtaining an ATO. The remaining Core Infrastructure capabilities operate under the NCPS, which received an ATO on September 6, 2019.

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.[6]

[6] NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, REQUEST FOR RECORDS DISPOSITION AUTHORITY, RECORDS SCHEDULE NUMBER DAA-0563-2013-0008, U.S. DEPARTMENT OF HOMELAND SECURITY, NATIONAL CYBERSECURITY PROTECTION SYSTEM (2015), 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.

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 PRA is not applicable to the information collected by NCPS core infrastructure capabilities.

Section 2.0 Characterization of the Information

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

CISA cybersecurity analysts may collect name, phone number, email address, and affiliation (e.g., company or agency name) from individuals both domestic and international who submit cyber threat incident report information via telephone, fax, or the Internet. In addition, user information is collected from CISA personnel who use the MOE and TS MOE to establish and maintain their accounts. This information includes name, email address, phone number, and organization.

Additionally, operational cybersecurity data may incidentally include PII. This PII is not intentionally captured but may be captured because it is a part of an email address, username, or found in files that are relevant to understanding cybersecurity threats.[7] If identified as not relevant, this information is deleted. Operational cybersecurity data is not retrieved by a personal identifier.

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

For cyber incident reporting, sources of information include individuals, private sector entities, and personnel working at other federal or state agencies. In addition, information is also received from international sources,[8] including individuals, companies and other nations' governments. As a practical matter, sources principally include federal government network security managers and those in the private sector who are interested and willing to contribute to the catalog of incidents or analysis of the incident, primarily those working within the cyber network defense community.

[7] *See supra* note 2.

[8] As noted above, the exchange of information on cybersecurity occurs between DHS, departments and agencies, intelligence agencies, state, local, tribal governments, private organizations, foreign computer security incident response teams, and the public. This sharing is done in accordance with MOAs or other types of information sharing agreements, as applicable.

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

CISA 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, operational uses of social media). This data is used to understand cyber events that are reported to CISA and for historical reference of similar incidents. CISA only uses commercial or publicly available data that is relevant to the CISA cybersecurity mission and does not use it for identifying individuals.

2.4 Discuss how accuracy of the data is ensured.

Where individuals voluntarily provide their name, email, phone number, and incident data, CISA cybersecurity analysts may call or email the individuals to verify their information, security data, or to follow-up on a reported cyber incident submitted by the individual or organization.

In order to assess the veracity of an incident that is reported to CISA, the analysts:

1) Capture incident data;
2) Verify the data through closed or open source research (e.g., Google, NCPS intrusion detection network flow data);
3) Contact the system owner;
4) Triage the incident, identify other affected parties and contact them; and
5) Work with the affected party or organization to identify mitigation strategies.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: NCPS core infrastructure capabilities may collect more data than is necessary, including PII, and due to the nature of how the data is collected, some information may be inaccurate or fraudulent.

Mitigation: This risk is mitigated. NCPS core infrastructure capabilities only collect data that is necessary to accomplish the CISA cybersecurity mission. For contact information collected from individuals to provide cyber incident reports, CISA collects the minimum information necessary directly from the individuals. For information collected from the person reporting the incident, analysts may attempt to confirm the integrity of the data received through the voluntary submissions by contacting the individual through phone or email. When provided, this includes the contact information of the person reporting the incident (if applicable), cyber incident data, which may include IP and host addresses and flow data, and actions taken to resolve the incident.

All data containing PII is managed in accordance with the appropriate CISA standard operating procedures (SOP) and information handling guidelines. All PII is reviewed prior to being included in any analytical products or other forms of dissemination. CISA 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, CISA SOPs and information handling guidelines provide safeguards for the marking, dissemination, and handling of the information.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

Information collected from cyber incident reporting is used to identify and respond to cybersecurity incidents and to generate reports for distribution on those incidents to DHS organizations, federal agencies, and other cybersecurity partners.

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 core infrastructure capabilities are not configured or used to complete queries based on PII. Queries are limited to data and cyber incident information necessary to identify trends and patterns in cyber threat indicators and disparate data sets.

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

No. Only CISA 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 core infrastructure capabilities will be used inappropriately.

Mitigation: This risk is mitigated. CISA cybersecurity analysts, as well as NCPS administrators and information assurance personnel, are trained on both DHS and CISA specific procedures for handling and safeguarding PII. Those personnel receive privacy training upon being hired and are required to take annual refresher training. In addition, CISA 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 core infrastructure 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[9] must sign Rules of Behavior that identify 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.

This PIA serves as notice of NCPS core infrastructure capabilities. Notice is also provided through previously published DHS cybersecurity-related PIAs.

If an individual reports a cyber incident by telephone, their contact information is not required. When submitting a cyber incident via email or through the CISA website, contact information is required. In those circumstances, notice and a banner are provided to the reporting individual regarding the potential uses of the information of the individual prior to their submission of the incident. Further notice is provided by the Privacy Policy available at the following site https://www.dhs.gov/privacy-policy.

The system of records notices applicable to the NCPS: DHS/ALL-016 Correspondence Records and DHS/ALL-004 General Information Technology Access Account Records Systems also provide notice of the collection of this type of personal information.

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

For incidents reported to CISA via telephone, individuals have the right to voluntarily provide (or decline to provide) their contact information when submitting information regarding a cyber-related incident or submitting a trouble ticket. If the submitter chooses to not provide such information, CISA will still process the report based on what information has been provided.

PII may be required in order to process or respond to queries made by individuals to the federal government, but it is not mandatory that an individual provide this information.

[9] 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.

In addition, all CISA personnel logging into an NCPS system are presented with an electronic notice that informs them that DHS computer systems are monitored. Users can accept or decline the terms of use.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a privacy risk that individuals reporting a cyber incident to CISA may not realize their PII is being retained or that an individual may choose not to read the notice or banner provided or be aware of the information collection occurring under the NCPS.

Mitigation: This risk is mitigated. For individuals reporting a cyber incident to CISA, a statement is included during the reporting process to ensure that the individual has adequate notice of the collection and the potential uses of the information. For example, if a report is taken through the phone, the call agent is required to give notice to the person that any information they provide is voluntary, and if they choose to provide information, their information will be used for limited purposes. Contact information is collected, although not required, in order for the researcher assigned to the code or incident to follow up with the original submitter should the information available be incomplete or inaccurate.

In the course of normal operations, it is possible that PII could be collected through the submission of suspicious code, spam, or malware. In the event this information is collected, CISA cybersecurity analysts are required to follow SOPs for the handling of this information.

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 core infrastructure capabilities only to protect information and information systems from cybersecurity risks. Data collected through NCPS core infrastructure capabilities is retained in accordance with the approved records retention schedule for the NCPS (DAA-0563-2013-0008). Core infrastructure 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. CISA cybersecurity analysts are required to review all data collected to determine whether PII is present and if it is necessary to analyze or understand the cybersecurity threat. CISA information handling guidelines and SOPs provide the procedures for the collection processing, retention, and dissemination of PII.

In addition, CISA has worked with the NARA to develop an approved records retention schedule for NCPS records (DAA-0563-2013-0008), which states that NCPS core infrastructure 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.

As part of its computer network security responsibilities, CISA generates 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 or entity that established the network connection that triggered an alert or who reported the cyber incident 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.

CISA also shares analysis, along with additional computer network security products, with its partners and constituents (federal departments and agencies, state, local, and tribal governments, industry, academia, the general public, and international partners) via its website: www.us-cert.gov.

Further, in accordance with its SOPs, CISA notifies law enforcement or an intelligence entity of cyber incidents of relevance to the mission, primary jurisdiction or other applicable authorities for action.

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

As applicable, the routine uses for the NCPS data, are governed by the DHS system of records notices titled, DHS/ALL-016 Correspondence Records, 83 Fed. Reg. 48645 (September 26, 2018) and DHS/All-004 General Information Technology Access Account Records Systems, 74 Fed. Reg. 49882 (September 29, 2009).

In addition to those disclosures generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act, all or a portion of the records of information contained in these systems may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. § 552a(b)(3).

6.3 Does the project place limitations on re-dissemination?

CISA 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 CISA Homeland Security Information Network portal. Some of the information disseminated to these partners may contain or be derived from NCPS core infrastructure data.

Cyber threat information received through NCPS core infrastructure 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 CISA leadership in advance of dissemination, in accordance with the appropriate CISA SOPs and information handling guidelines. Additionally, CISA typically restricts dissemination and re-dissemination of cyber threat information using the Traffic Light Protocol.[10]

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

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

No formal reports disseminated via the 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. If PII must be released, it is released in accordance with the Privacy Act of 1974,[11] appropriate CISA SOPs, and information handling guidelines, and with the authorization and/or written approval of CISA leadership.[12]

6.5 Privacy Impact Analysis: Related to Information Sharing

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

Mitigation: This risk is mitigated. Unauthorized disclosure is mitigated through various means, including encrypting the information and limiting who has access to the information. CISA maintains specific SOPs and information handling guidelines governing the use of information, including PII. All PII is reviewed and that information is only shared if it is determined to be

[10] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA), TRAFFIC LIGHT PROTOCOL (TLP) DEFINITIONS AND USAGE, https://www.us-cert.gov/tlp (last visited July 26, 2020).
[11] 5 U.S.C. § 552a.
[12] 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.

analytically relevant to a particular cyber threat. If a report containing PII is developed or modified for multiple audiences, each version is reviewed for appropriate markings.

Appropriate CISA 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 guidelines and information identifying sources and methods from all CISA 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?

Individuals seeking access to any record containing information that is part of a DHS system of records may submit a Freedom of 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. Please write to:

CISA FOIA Officer
245 Murray Lane SW
Washington, D.C. 20528-0380

Individuals may also make information inquiries to CISAFOIA@hq.dhs.gov.

The release of information is subject to standard FOIA exemptions and, given the nature of the cyber threat information contained in the NCPS, CISA may not always permit individuals to gain access or grant 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 DHS Correspondence Records and GITAARS SORNs.

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

Individuals seeking to amend the accuracy of the content of a record containing information that is part of a DHS system of record 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. Please write to:

CISA FOIA Officer
245 Murray Lane SW
Washington, D.C. 20528-0380

Individuals may also make information inquiries to CISAFOIA@hq.dhs.gov.

The release of information is subject to standard FOIA exemptions and, given the nature of the cyber threat information contained in the NCPS, CISA may not always permit individuals to gain access or grant 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 DHS Correspondence Records and GITAARS SORNs.

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. The SORNs applicable to NCPS also provide notice of the redress procedures for this type of information.

7.4 Privacy Impact Analysis: Related to Redress

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

Mitigation: This risk is mitigated. Although it may be difficult in some instances to provide adequate redress due to the nature of the system, CISA has measures in place to provide individuals with the ability to request access to and correction of records. These procedures are described in Sections 7.1, 7.2, and 7.3 above. Additionally, this PIA and the applicable SORNs provide notice for individuals seeking redress related to NCPS records.

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?

CISA has developed SOPs and information handling guidelines that govern the collection, handling, and dissemination of cybersecurity information. In addition, the CISA Office of Privacy performs bi-annual privacy oversight reviews to ensure that cybersecurity information is handled in accordance with the appropriate procedures and guidelines.

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, CISA 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 network flow 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?

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. 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 by the either the user for account updates or by a current NCPS user for new accounts. The functional area managers validate the need to know in the approval process.

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,[13] accounts are subject to disablement for non-compliance. User accounts are disabled after 30 days of inactivity or promptly upon departure from the organization.

[13] 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*. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, DHS 4300A SENSITIVE SYSTEMS HANDBOOK, *available at* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook (last accessed July 26, 2020).

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 developed 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, CISA Office of the Chief 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

Martin Gross
Cybersecurity Division
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
(703) 235-2853

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Dena Kozanas
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717