Privacy Impact Assessment

for the

Use of Administrative Subpoenas for Cybersecurity Vulnerability Identification and Notification

DHS Reference No. DHS/CISA/PIA-038

May 11, 2021

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Division (CSD) has established a process that permits CISA, pursuant to statutory authority,[1] the use of administrative subpoenas for cybersecurity vulnerability identification and notification. This process allows CISA to issue administrative subpoenas and receive customer or subscriber contact information from service providers to identify and notify owners or operators of covered systems and devices[2] related to critical infrastructure that have a specific security vulnerability. CISA is conducting this Privacy Impact Assessment (PIA) because responses to administrative subpoenas will include the personally identifiable information (PII) of individuals identified by subpoenaed service providers, such as Internet Service Providers (ISPs), as relevant points of contact.

Overview

One of CISA's responsibilities is protecting critical infrastructure by sharing information about vulnerabilities that—if left unmitigated—leave critical infrastructure susceptible to attack by our nation's most advanced adversaries. To fulfill this responsibility, CISA has authority to share timely and actionable cybersecurity risk information with critical infrastructure partners to help them protect their systems. Unfortunately, there are instances where cybersecurity vulnerabilities on Internet-connected systems are identified, but CISA is unable to determine the identity of the owner or operator of the system and therefore cannot contact the entity to advise it of the vulnerability. Many of the vulnerable systems CISA finds are identified only by a numerical Internet protocol (IP) address. Issuing administrative subpoenas to service providers with the relevant customer or subscriber information, typically ISPs, allows CISA to receive the vulnerable entity's contact information, which will include personally identifiable information (PII) such as the name, phone number, and address. Receiving this information from subpoena responses enables CISA to contact the entity, inform them of the potential risk, and offer mitigation advice or assistance.

All information related to administrative subpoenas will be manually entered, updated, and tracked through CISA's Incident and Event Management System, Tardis. Prior to issuing a subpoena, CISA must document the specific vulnerability identified on the Internet-connected covered system or device, the reason to believe the device or system is related to critical

[1] *See* the National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 1716, 134 Stat. 3388, 4094-4099 (2021), codified in 6 U.S.C. § 659.

[2] "Covered device or system" means a device or system commonly used to perform industrial, commercial, scientific, or governmental functions or processes that relate to critical infrastructure, including operational and industrial control systems, distributed control systems, and programmable logic controllers; and does not include personal devices and systems, such as consumer mobile devices, home computers, residential wireless routers, or residential Internet-enabled consumer devices.

infrastructure and not a personal device or system, and a critical infrastructure risk assessment. Additionally, CISA must document the steps previously taken to identify the owner or operator of the vulnerable system. All requests for subpoenas are reviewed by the CISA Office of the Chief Counsel (OCC) and the CISA Office of the Chief Privacy Officer (OCPO) to ensure all the gating criteria listed above are met. In the interest of avoiding interference with ongoing law enforcement investigations, and as required by law, CISA also coordinates the issuance of any such subpoenas with the Department of Justice, including the Federal Bureau of Investigation (FBI).

During this coordination, CISA will provide the FBI the opportunity to object to the issuance of a subpoena. This will be done via email with a list of the vulnerable IP addresses and a description of the vulnerability associated with those IP addresses. If the FBI/National Cyber Investigative Joint Task Force (NCIJTF) objects to the issuance of a subpoena, CISA and FBI/NCIJTF will confer to seek a resolution, which may include not pursuing a subpoena. If a resolution cannot be reached at the staff level, the issue will be escalated to CISA and FBI leadership to seek a resolution by mutual agreement.

The subpoenas will be issued to providers of electronic communication or remote computing services to the public, such as ISPs, that have relevant customer or subscriber information to identify the owners or operators of covered devices or systems with a specific security vulnerability, often identified through their IP address. CISA will receive information from these subpoenaed entities. In the event the customer or subscriber identified in the subpoena response is not the most appropriate individual at the vulnerable entity, CISA may ask for a referral from the initial identified individual to pursue more accurate information in order to identify the owner or operator of the covered device or system.

Once a subpoena is approved and issued and CISA has received a response, CISA must notify the at-risk entity identified by the subpoena no later than seven (7) days after receiving the customer or subscriber information. The notification to the at-risk entity includes a discussion or statement that responding to or engaging with CISA is voluntary, and information about the process through which CISA identifies security vulnerabilities. CISA places no requirement on the entity to take any action on the identified vulnerability.

Law requires the destruction of information determined to be unrelated to critical infrastructure immediately upon providing notice to the entity, and the destruction of all PII not later than six (6) months after the date on which the subpoena response is received.[3] When PII relates to an individual, the individual may consent to CISA retaining his or her information for future communication --- but this consent will result in a new record. Upon consent for retention, the contact information will be retained in accordance with DHS/ALL/PIA-006 DHS General

[3] 6 U.S.C. § 659(o)(7)(C).

Contact Lists[4] and DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists Systems.[5]

All information obtained through a subpoena must only be shared with (1) another federal department or agency for a cybersecurity purpose[6] under the limited circumstances described below or (2) with the Department of Justice for enforcement of the subpoena. CISA may share nonpublic information obtained through the subpoena with a federal agency if CISA identifies or is notified of a cybersecurity incident involving the entity and the incident is related to the vulnerability which led to the issuance of the subpoena in the first place; CISA determines that sharing the information is necessary to allow the federal department or agency to take a law enforcement or national security action or action related to mitigating or otherwise resolving such incident; and the entity is notified (to the extent practicable consistent with national security or law enforcement interests), and consents to the sharing (although exceptions to the consent requirement may apply).

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?

- *Homeland Security Act of 2002,[7] as amended*, establishes and authorizes various functions for CISA's cybersecurity operations, including its authority to share information related to cybersecurity risks and incidents with federal and non-federal entities. This includes subsection (o) of Section 2209 of the Homeland Security Act, as amended, (6 U.S.C. 659(o)), which was enacted by Section 1716 of the National Defense Authorization Act for Fiscal Year 2021 and grants CISA the authority to issue administrative subpoenas, subject to statutory limitations.

- *Presidential Policy Directive (PPD) 21[8]* advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. The directive instructs the federal government to work with critical infrastructure owners and

[4] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR GENERAL CONTACT LISTS, DHS/ALL/PIA-007 (2007 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.
[5] *See* DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, 73 Fed. Reg. 71659 (Nov. 25, 2008), *available at* https://www.dhs.gov/system-records-notices-sorns
[6] "Cybersecurity purpose" means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability. *See* Cybersecurity Information Sharing 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)).
[7] *See* Title XXII of the Homeland Security Act of 2002 (6 U.S.C. §§ 651 – 674, esp § 2209 of the Homeland Security Act (6 U.S.C. § 659(c)(6)).
[8] Presidential Policy Directive-21 (PPD-21) of February 12, 2013 (Critical Infrastructure Security and Resilience)

operators and state, local, tribal and territorial (SLTT) governments to take proactive steps to manage risk and strengthen the security and resilience of the Nation's critical infrastructure.

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

Information received through the issuing of administrative subpoenas can be retrieved by a personal identifier. When personally identifiable information is retrieved in this way, it meets the requirements of the Privacy Act, requiring a SORN to be published in the Federal Register. Thus, CISA recently published DHS/CISA-005 Administrative Subpoenas for Cybersecurity Vulnerability Identification and Notification System of Records.[9]

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

Administrative subpoena issuance will be tracked through CISA's Incident and Event Management System, known as Tardis. A system security plan and Authorization to Operate (ATO) has been completed for Tardis.

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

A records retention schedule has not yet been approved by NARA. However the legislation granting CISA the authority to subpoena entities for the production of this information requires that all PII received through a subpoena response be deleted no later than six (6) months after the date which CISA received the information, unless otherwise agreed to by the individual identified by the subpoena respondent. Additionally, the legislation requires the destruction of information determined to be unrelated to critical infrastructure immediately upon providing notice to the entity.

[9] *See* DHS/CISA-005 Administrative Subpoenas for Cybersecurity Vulnerability Identification and Notification System of Records, 86 Fed. Reg. 17616 (April 5, 2021), *available at* https://www.dhs.gov/system-records-notices-sorns.

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.

This information is not covered by the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

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

Information received through administrative subpoenas are limited to the categories set forth in subparagraphs (A), (B), (D), and (E) of section 2703(c)(2) of title 18, United States Code. These are the name, address, length of service (including start date), types of services utilized, and telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address of the subscriber or customer whose information is maintained by an electronic communication or remote computing service provider. Additionally, the system will also contain the IP address of the covered device or system with the specific security vulnerability used to identify the vulnerable entity, CISA-created ticket number for internal tracking purposes and the individual's position, title, or organizational affiliation.

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

Information is received from a subpoenaed individual, partnership, corporation, association, or entity. Information may also be obtained through public sources or contact with an individual identified through the issuing of a subpoena.

The subpoenas will be issued to providers of electronic communication or remote computing services to the public, such as ISPs, that have relevant customer or subscriber information to identify the owners or operators of covered devices or systems with a specific cybersecurity vulnerability, often identified through their IP address. CISA will receive information from these subpoenaed entities. In the event the customer or subscriber identified in the subpoena response is not the most appropriate individual at the vulnerable entity, CISA may ask for a referral to contact the correct individual.

The information maintained for the purposes of identifying an entity needing to be subpoenaed, such as the IP address, will be obtained through publicly available information. Subpoenas can only be issued when a device or system connected to the Internet is found to have a specific security vulnerability. These vulnerable devices or systems are identified through their IP address which is accessible via the Internet.

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

Prior to the issuing of a subpoena, CSD collects publicly available data about a vulnerable entity using online tools such as Shodan, WHOIS, Censys, and Google Dorking. These online tools allow CISA to identify the IP address of Internet-connected systems with a cybersecurity vulnerability. CISA will also use these tools to attempt to identify the owner or operator of the vulnerable entity. If CISA can successfully identify the owner or operator, then an administrative subpoena will not be issued. Therefore, no information used to identify an individual and maintained as part of an administrative subpoena is collected or verified from commercial or publicly available services.

2.4 Discuss how accuracy of the data is ensured.

The subpoenas will be issued to providers of electronic communication or remote computing services, such as ISPs, that have relevant customer or subscriber information to identify the owners or operators of covered devices or systems. Once CISA receives a subpoena response, the agency has seven (7) days to notify the entity or individual identified by the information received. If information received in the subpoena response is not accurate the information will be immediately destroyed. In this event CISA may ask for a referral from the initial identified individual, prior to destruction, to pursue more accurate information in order to identify the owner or operator of the covered device or system. This ensures that only relevant and accurate data is maintained.

The ISP is reasonably believed to have the most up-to-date information because an entity is being identified through the Internet as utilizing their service.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: Information received through the subpoena may no longer be accurate or may not be the information CISA needs to contact the at-risk entity in a timely manner.

Mitigation: The risk is mitigated. Subpoena responses only provide information that is necessary to identify an individual and notify the at-risk entity. When received, this information must be acted on within seven (7) days of receipt. If the information is determined to be incorrect and will not allow CISA to provide the necessary notification, the information will no longer serve a cybersecurity purpose and must be deleted.

All data containing PII is managed in accordance with the appropriate CISA standard operating procedures (SOP) and cybersecurity information handling guidelines which provide

safeguards for the marking, dissemination, and handling of the information. CISA information handling guidelines require that PII be removed or replaced with a generic label whenever it is not necessary.

Privacy Risk: Responses to subpoenas may contain more information than requested.

Mitigation: The risk is mitigated. If information provided in response to a subpoena is determined to be unrelated to critical infrastructure or does not serve a cybersecurity purpose, it must be deleted immediately upon providing notice to the at-risk entity. The Electronic Communications Privacy Act (ECPA) limits the information that electronic communication and remote computing service providers can provide to a governmental entity in response to an administrative subpoena to only six categories of information. CISA's authority to issue administrative subpoenas limits the information CISA can receive to only four of the six categories set out in ECPA,[10] as described in Section 2.1.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

Information received through responses to administrative subpoenas is used to identify and contact the owner or operator of a covered device or system with a security vulnerability which CISA has reason to believe is related to critical infrastructure. When CISA receives a response to a subpoena, CISA will contact the individual identified and include, to the extent practicable, information regarding the process through which CISA identifies security vulnerabilities.

In the event the individual contacted consents to CISA retaining his or her contact information for future communication with CISA, the individual's name, email address, phone number, and address, as applicable, will be retained as a separate record. If the individual consents to this, the information will be retained in accordance with the DHS/ALL/PIA-006 DHS General Contact Lists[11] and DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists Systems.[12]

[10] *See* 6 U.S.C. § 659(o)(2)(B).
[11] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR GENERAL CONTACT LISTS, DHS/ALL/PIA-007 (2007 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.
[12] *See* DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, 73 Fed. Reg. 71659 (Nov. 25, 2008), *available at* https://www.dhs.gov/system-records-notices-sorns.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No, the administrative subpoena process does not use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly. No new data will be created with the information received through the subpoena responses to allow for any other types of data, matching, relational analysis, scoring, reporting, or pattern analysis.

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

No other DHS component will have assigned roles or responsibilities in the administrative subpoena process.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information received through a subpoena response will be used or disclosed inappropriately.

Mitigation: This risk is mitigated. All CISA employees with access to the IT system that manages the administrative subpoena process 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 information handling guidelines and practices for the identification of sensitive information and the proper handling, safeguarding, and minimization of PII, and defines the terms of use for specifically identified roles and responsibilities. Additionally, all information received must be used for a cybersecurity purpose.

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.

Notice is provided through the publication of the legislation, information regarding internal processes and procedures published on the CISA website (www.CISA.gov), this PIA, and through the recently published SORN in the Federal Register. Because CISA is unable to identify the individual through other means, providing direct notice to an individual at the point of collection is not possible.

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

Information received through a subpoena response may only be used for limited cybersecurity purposes including to notify the individual identified of the specific vulnerability on the covered device or system.

The individual does not have the opportunity to initially opt out or decline to provide information; however, once contacted by CISA, the individual may consent to CISA retaining his or her contact information for future communications. If the individual provides this explicit consent, the information will be retained in accordance with DHS/ALL/PIA-006 DHS General Contact Lists. If the individual does not consent to future contact with CISA, the system will destroy the individual's PII not later than six (6) months after the date which the information was received.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that an individual may not be aware of his or her information being provided to CISA through responses to administrative subpoenas.

Mitigation: This risk is partially mitigated. Through the publishing of information regarding CISA's internal processes and procedures, this PIA, and the recently published SORN, the public is provided notice of this process and collection of PII. However, individual notice is not possible prior to CISA receiving information through an administrative subpoena. Upon receipt of PII in a subpoena response, CISA must notify the individual within seven (7) days of receipt. This limits the time CISA maintains an individual's PII without his or her knowledge.

Section 5.0 Data Retention by the Project

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

Information received through a subpoena response is retained for the purposes of identifying and contacting the owner or operator of a covered device or system with a security vulnerability which CISA has reason to believe is related to critical infrastructure. In accordance with the legal authority in Question 1.1, any personally identifiable information must be destroyed not later than 6 months after the date on which CISA received the information through a subpoena response. Additionally, information received through a subpoena that CISA determines is unrelated to critical infrastructure must be destroyed immediately upon providing notice to the at-risk entity.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk PII may be retained beyond the 6-month authority.

Mitigation: The risk is mitigated. The incident and event management system which will maintain the information related to the subpoena will automatically delete all PII (unless consent for retention has been obtained) 6 months after the date on which CISA received the information.

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.

CISA may share nonpublic information of the at-risk entity via phone call, email, or other secure method with a federal agency only if the requirements of 6 U.S.C. § 659(o)(7)(a) are met. These requirements include (1) that CISA identifies or is notified of a cybersecurity incident involving the entity and relating to the vulnerability which led to the issuance of the subpoena; (2) CISA determines that sharing is necessary to allow the federal agency to take law enforcement or national security action or actions related to mitigating or otherwise resolving such incident; (3) the entity is notified (to the extent practicable consistent with national security or law enforcement interests); and (4) the entity consents to the sharing (although consent shall not be required if another federal department or agency identifies the entity to CISA in connection with a suspected cybersecurity incident). Additionally, this sharing must occur solely for a cybersecurity purpose.

CISA may also share nonpublic information with the Department of Justice for the purposes of enforcing a subpoena. This sharing would likely occur prior to the subpoena response and likely would not include any information identifying an individual.

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

The routine use in the recently published SORN permits CISA to share the nonpublic information with the Department of Justice for the purpose of enforcing such subpoena in non-compliance circumstances, and with a federal agency only if the requirements of 6 U.S.C. § 659(o)(7)(A) are met.

6.3 Does the project place limitations on re-dissemination?

Yes, information may only be shared in limited circumstances for specific purposes, as set out in 6 U.S.C. §§ 659(o)(7)(A) and 659(o)(13).

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

All information sharing actions are recorded in Tardis, the Incident and Event Management System which will maintain all the information related to the administrative subpoena process.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information will be shared with another federal agency which does not fit the purposes outlined in the legal authority.

Mitigation: The risk is mitigated. CISA maintains specific SOPs and cybersecurity information handling guidelines governing the use of information, including PII. All PII is reviewed and information is only shared if it is determined to meet the conditions of 6 U.S.C. § 659(o)(7)(A). Additionally, all requests for subpoenas are reviewed by CISA OCC and the CISA OCPO.

Section 7.0 Redress

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

As outlined in the recently published SORN referenced, individuals seeking to access their information maintained as a part of the administrative subpoena process may submit a Freedom of Information Act (FOIA) or Privacy Act request to the DHS/CISA FOIA Officer. Individuals may obtain instructions on how to submit a FOIA/Privacy Act request at https://www.dhs.gov/freedom-information-act-foia. Please write to:

The Privacy Office
Privacy Office, Mail Stop 0655
U.S. Department of Homeland Security
2707 Martin Luther King Jr. Ave SE
Washington, D.C. 20528-065

Individuals may also make information inquiries to CISAFOIA@hq.dhs.gov. The release of information is subject to standard FOIA exemptions.

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 the administrative subpoena process may submit a FOIA or Privacy Act request to the DHS/CISA FOIA Officer. Individuals may obtain instructions on how to submit a FOIA/Privacy Act request at https://www.dhs.gov/freedom-information-act-foia. Please write to:

The Privacy Office
Privacy Office, Mail Stop 0655
U.S. Department of Homeland Security
2707 Martin Luther King Jr. Ave SE
Washington, D.C. 20528-065

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

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

This PIA and the associated SORN 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 related to the administrative subpoena process.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will want to seek redress for their PII CISA receives through an administrative subpoena.

Mitigation: The risk is mitigated. While CISA is unable to grant access or correct the PII that is maintained by an ISP, if individuals wish to request access to or correct the records CISA obtains through an administrative subpoena, they may follow the procedures described in this section. Additionally, this PIA and the associated SORN provide notice for individuals seeking redress related to records. However, due to the limited retention periods of this data, CISA may not be able to provide records beyond a certain timeframe.

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?

Prior to issuing a subpoena to an ISP, both CISA OCC and CISA OCPO review the subpoena request to ensure CISA documented the specific vulnerability identified on the Internet-connected covered system or device, the reason to believe the device or system is related to critical infrastructure and not a personal device or system, and a critical infrastructure risk assessment.

OCPO advised on and reviewed the building of the dashboard in Tardis where all PII received through an administrative subpoena will be maintained. OCPO's participation in this process ensured all privacy requirements are met and all information is used in accordance with the stated practices in this PIA.

Additionally, pursuant to 6 U.S.C. § 659(o)(8), the CISA Privacy Officer is required to

review the internal procedures after one (1) year to ensure all internal procedures are consistent with fair information practices. This report will allow CISA to determine adherence to the stated practices in this PIA.

CISA has developed SOPs and information handling guidelines that govern the collection, handling, and dissemination of cybersecurity information. These SOPs and guidelines apply to all PII obtained through an administrative subpoena. In addition, OCPO 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.

Law requires the CISA Director to establish training on CISA's internal procedures regarding subpoenas issued under the statute. CISA is currently in the process of developing trainings to satisfy this requirement. In addition, all CISA employees are required to complete annual Privacy Awareness Training and CISA cybersecurity analysts are required to participate in regular role-based training on the procedures and guidelines for the handling of cybersecurity information.

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 employees in the administrative subpoena process must have a valid need to access Tardis and receive only the type of access required to meet their specific job duties and responsibilities. Employees are assigned the relevant system role within Tardis needed to successfully fulfill their job duties and responsibilities. System roles are pre-defined and approved by functional managers within CISA. If personnel require a system role that exceeds their usual job duties and responsibilities, their access must be approved by a functional manager within CISA. Additionally, users are required to complete security awareness training annually. Per DHS 4300A, Policy 13,[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.

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 procedures for coordination between CISA and the Department of Justice for

[13] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, DHS SENSITIVE SYSTEMS POLICY DIRECTIVE 4300A (2017), *available at* https://www.dhs.gov/privacy-policy-guidance.

deconfliction with FBI/NCIJTF were reviewed by program managers from both agencies, system owners for Tardis, OCC, and OCPO. The standard operating procedures strictly outlining restrictions on sharing and handling of information were also reviewed by CISA program managers, Tardis system owners, OCC, and OCPO.

The uses and sharing of the information obtained through and used by administrative subpoenas is strictly limited and there will be no future administrative subpoena information sharing agreements, MOUs, new uses of information, or new access to the system by organizations within DHS or outside.

Contact Official

Christine Cunningham
Branch Chief of Integration
Cybersecurity and Infrastructure Security Agency, Cybersecurity Division
christine.cunningham@cisa.dhs.gov

Responsible Official

Eric Goldstein
Executive Assistant Director for Cybersecurity
Cybersecurity and Infrastructure Security Agency

Approval Signature

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

_____

Lynn Parker Dupree
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717