Privacy Review of Administrative Subpoenas

Results on Review of Procedures

July 07, 2022

Homeland Security

Cybersecurity and Infrastructure Security Agency (CISA)

Message from the Chief Privacy Officer of the Cybersecurity and Infrastructure Security Agency

July 07, 2022

I am pleased to present the following report, "Privacy Review of Administrative Subpoenas," which has been prepared by the Office of the Chief Privacy Officer of the Cybersecurity and Infrastructure Security Agency (CISA).

This document has been compiled pursuant to a requirement in subsection (p)(9) of Section 2209 of the Homeland Security Act, as amended.

This report is being provided to the following Members of Congress:

The Honorable Bennie G. Thompson
Chairman, House Committee on Homeland Security

The Honorable John Katko
Ranking Member, House Committee on Homeland Security

The Honorable Gary C. Peters
Chairman, Senate Committee on Homeland Security and Governmental Affairs

The Honorable Rob Portman
Ranking Member, Senate Committee on Homeland Security and Governmental Affairs

Inquiries relating to this report may be directed to the CISA Office of Legislative Affairs at (202) 819-2612.

Sincerely,

James Burd
Chief Privacy Officer
Cybersecurity and Infrastructure Security Agency

Executive Summary

The development of the Cybersecurity and Infrastructure Security Agency (CISA) administrative subpoena processes included members of CISA's Office of the Chief Privacy Officer (OCPO) from inception to ensure privacy was a priority throughout the use of administrative subpoenas to identify and notify vulnerable entities. This "Privacy Review of Administrative Subpoenas" is a statutory requirement distinct from the statutory requirement for an annual report on the use of administrative subpoenas. This separate report highlights the importance of maintaining the privacy of individuals and entities throughout the subpoena process – from identification of a vulnerable device through issuance of an administrative subpoena to entity notification and mitigation of the vulnerability.

The "Privacy Review of Administrative Subpoenas" details how the agency ensures the procedures of the administrative subpoena process are consistent with fair information practices and how the agency complies with those procedures. For the purposes of this report, the fair information practices used are the Fair Information Practice Principles set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace. This report includes a review of all 70 administrative subpoenas initiated in calendar year 2021 for vulnerable systems or devices identified. This number is inclusive of the 47 administrative subpoenas which were initiated and issued within calendar year 2021 as reported in the "Administrative Subpoena Annual Report: Calendar Year 2021 Report to Congress." This review to ensure compliance with internal procedures was conducted by OCPO employees who were not involved in the creation of the procedures to help ensure an independent review.

This report includes an overview of the CISA administrative subpoena process, a detailed alignment of the procedures with fair information practices, the methodology of how CISA OCPO reviewed the procedures and operations of the agency for compliance with the procedures, and the results of that review.

Privacy Review of Administrative Subpoenas

Table of Contents

I. Legislative Language

Subsection (p)(9) of Section 2209 of the Homeland Security Act, as amended, include(s) the following requirement:

> (9) REVIEW OF PROCEDURES.–Not later than 1 year after the date of the enactment of this subsection, the Privacy Officer of the Agency shall –
>
> (A) review the internal procedures established pursuant to paragraph (7) to ensure that–
>
> (i) such procedures are consistent with fair information practices; and
>
> (ii) the operations of the Agency comply with such procedures; and
>
> (B) notify the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives of the results of the review under subparagraph (A);

II. Background

The Cybersecurity and Infrastructure Security Agency (CISA) leads national cybersecurity asset response activities, including understanding, assessing, and reducing risk to the cyber and physical infrastructure of the United States. As part of this mission to help protect critical infrastructure from cybersecurity risks, CISA aims to share information about vulnerabilities that—if left unmitigated—could leave critical infrastructure susceptible to attack by threat actors. CISA has authority to share timely and actionable cybersecurity risk information with federal and non-federal partners to help protect their systems and devices. There are, however, instances in which cybersecurity vulnerabilities on Internet-connected systems are identified, but CISA analysts are 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 devices and systems CISA finds are identifiable only by a numerical Internet protocol (IP) address. Entities such as internet service providers (ISPs) can identify the owners or operators of the vulnerable devices but are often prohibited by law or contract from disclosing the information to the government in the absence of compulsory legal process. Issuing administrative subpoenas to service providers, typically ISPs, with the relevant customer or subscriber information has enabled CISA to obtain the contact information of vulnerable entities. Although the contact information obtained through the subpoena process sometimes includes not just business entity information but also personally identifiable information (PII) of an individual associated with the entity such as an individual's name, telephone number, and address, receiving this information has enabled CISA to contact vulnerable entities, inform them of the potential risk, and offer mitigation guidance.

The statute that authorized CISA to issue administrative subpoenas required the development of internal procedures for issuing an administrative subpoena. The statute specifically requires the procedures to address the protection of and restriction on dissemination of non-public information obtained through a subpoena, which may at times include PII. Additionally, administrative subpoenas may only seek specific data elements and, once received, only allow for retaining PII for a specified timeframe, unless consent is granted for CISA to retain the PII longer. The drafters of the authority recognized the importance of safeguarding privacy throughout the subpoena process.

Since the granting of this authority, the CISA Office of the Chief Privacy Officer (OCPO) has been involved in the development of the administrative subpoena process, taking a leading role to ensure that the drafted procedures aligned with fair information practices and that the agency complied with them. OCPO continues to actively work with internal stakeholders to ensure compliance with statutory requirements and the success of the program. OCPO reviews every subpoena request when it is submitted to ensure that the request documents sufficient reason to believe the vulnerability is related to critical infrastructure and the device is not a personal device and that CISA has taken all other reasonable steps to identify the owner and operator. Consistent with Subsection (p)(9), OCPO also reviews CISA's adherence to the process, including reviewing the timely deletion of PII when appropriate. The authorizing statute places restrictions on the retention of all PII obtained through subpoenas unless otherwise agreed to by the individual identified in the subpoena response.

As part of this review, OCPO has concluded that the procedures created for the issuance of administrative subpoenas are indeed consistent with fair information practices. Additionally, OCPO conducted a review and audit of CISA's adherence to the procedures using staff members who were not a part of the development of the administrative subpoena process nor participate in its day-to-day operations. The review determined that all subpoena requests documented sufficient reason to believe that vulnerable devices for which owner or operator information was being subpoenaed were related to critical infrastructure and not personal devices, and that CISA had taken all other reasonable steps to identify the owner and operator.

Furthermore, OCPO found that the administrative subpoena procedures resulted in the timely deletion of PII belonging to individuals, when appropriate, and that CISA took the necessary steps to obtain consent from individuals for retaining their PII beyond the statutorily prescribed 6-month retention limit.

III. Review of Alignment with Fair Information Practices

Though there are different articulations, the Fair Information Practice Principles (FIPP)[1] generally form the widely accepted framework of defining principles to be used in the evaluation and consideration of systems, processes, or programs that affect individual privacy. The FIPPs shaped CISA's implementation of subsection (p) of Section 2209 of the Homeland Security Act, as amended, for the development of internal administrative subpoena procedures from the beginning, as demonstrated in the subparagraphs below.

TRANSPARENCY

Definition: *Being transparent and notifying individuals regarding collection, use, dissemination, and maintenance of PII.*

Alignment: CISA's procedures are aligned with the Transparency FIPP in numerous ways. First, in the course of providing notification to the vulnerable entity, CISA's procedures require CISA analysts to provide transparency on how CISA identified the security vulnerability and explicitly state that future communications with CISA are completely voluntary. Additionally, information regarding CISA's procedures has been published on CISA's public-facing website (https://www.cisa.gov/cisa-administrative-subpoena) to notify individuals of the administrative subpoena process. Further, CISA's procedures informed the completion of a published Privacy Impact Assessment (PIA) titled "DHS/CISA/PIA-038: Use of Administrative Subpoenas for Cybersecurity Vulnerability Identification and Notification"[2] and a System of Records Notice titled "DHS/CISA-005: Administrative Subpoenas for Cybersecurity Vulnerability Identification and Notification System of Records"[3] to fully describe the receipt, retention, and use of PII in the course of administering the administrative subpoena process.

INDIVIDUAL PARTICIPATION

Definition: *Involving the individual in the process of using PII; to the extent practicable, seeking individual consent for the collection, use, dissemination, and maintenance of PII; and providing mechanisms for appropriate access, correction, and redress regarding use of PII.*

Alignment: Given the nature of the administrative subpoena's purpose, individual participation— including the opportunity to opt out or decline to provide information prior to or at the point of collection—is not possible. However, upon receipt of an individual's PII in a subpoena response, CISA's procedures require the individual identified to be notified within 7 days of receipt. This procedure aligns with the Individual Participation FIPP because it limits the time CISA maintains an individual's PII without his or her knowledge. Additionally, once

---

[1] This report analyzes the FIPPs as articulated in Appendix A of the National Strategy for Trusted Identities in Cyberspace, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf. While this articulation differs from that in Office of Management and Budget Circular A-130, *Managing Information as a Strategic Resource*, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf, which applies to all Federal agencies, CISA believes there is no substance lost between the two. In particular, OMB's *Access and Amendment* FIPP is captured in the *Individual Participation* FIPP here, and OMB's *Authority* FIPP is captured in the *Purpose Specification* FIPP.

[2] DHS/CISA/PIA-038 Use of Administrative Subpoenas for Cybersecurity Vulnerability Identification and Notification | Homeland Security

[3] DHS/CISA-005 Administrative Subpoenas for Cybersecurity Vulnerability Identification and Notification System of Records

contact with an individual is made, CISA's procedures require CISA analysts to ask the individual for consent for CISA to retain their information for future contact. If the individual does not consent to this retention, the procedures require CISA to delete the PII no later than 6 months after receipt.

PURPOSE SPECIFICATION

Definition: *Specifically articulating the authority that permits the collection of PII and specifically articulating the purpose or purposes for which the PII is intended to be used.*
Alignment: CISA is granted the administrative subpoena authority by subsection (p) of Section 2209 of the Homeland Security Act of 2002, as amended. This authority specifies the conditions under which CISA can issue an administrative subpoena and how the received information must be handled. CISA's procedures align with the Purpose Specification FIPP because they ensure each condition is met by requiring all subpoena requests to sufficiently document CISA's reason to believe the vulnerability is related to critical infrastructure; CISA's reason to believe the device or system is an enterprise device or system, not a personal one; and the efforts taken to identify the owner prior to issuing a subpoena. As required by the procedures, subpoena requests undergo multiple layers of review, including by the requesting branch's chief or designee, the Office of the Chief Counsel (OCC), and OCPO.

DATA MINIMIZATION

Definition: *Only collecting PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as necessary to fulfill the specified purpose(s).*
Alignment: Information received through a subpoena response is retained for the purposes of identifying and contacting the owner or operator of the identified vulnerable device or system. The type of information requested through a subpoena is limited to name, address, length of service (including start date), types of services utilized, and telephone or instrument number or other subscriber number or identity. CISA's procedures align with the Data Minimization FIPP because they require PII to be retained for no longer than 6 months, after which time it is automatically purged unless the individual consents to CISA retaining the information for the purposes of receiving future communication. Finally, the procedures require any non-public information obtained through a subpoena response to be destroyed immediately upon providing notice to the entity if CISA determines that the information is not related to critical infrastructure.

USE LIMITATION

Definition: *Using PII solely for the purpose(s) specified in the notice and sharing PII for a purpose compatible for the purpose for which the PII was collected.*
Alignment: CISA's procedures align with the Use Limitation FIPP because once information is received through a subpoena, CISA's procedures stipulate how information can be used and how to determine if the information can be shared. For example, if CISA determines the information received through a subpoena is unrelated to critical infrastructure, CISA's procedures require that the information from the subpoena response is destroyed upon providing notice to the vulnerable entity. Additionally, CISA's procedures require that CISA shall only use the information obtained through the administrative subpoena for a cybersecurity purpose. Further, CISA's procedures set out the specific conditions under which CISA can externally share non-

public information obtained through subpoenas. Per the procedures, these conditions are required to be met prior to sharing any information.

DATA QUALITY AND INTEGRITY

Definition: *Ensuring, to the extent practicable, that PII is accurate, relevant, timely, and complete.*

Alignment: All data received through the administrative subpoena process is provided by subpoena recipients and its quality is dependent on those entities. However, CISA's procedures align with the Data Quality and Integrity FIPP because once received, the procedures require CISA analysts to contact the vulnerable entity within 7 days of receipt. This ensures vulnerable entities are contacted within a reasonable period of time, while also reducing the likelihood that the identified point of contact or contact information will change before CISA contacts the entity.

SECURITY

Definition: *Protecting PII through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.*

Alignment: CISA's procedures align with the Security FIPP in that they require CISA to store and archive all information related to the administrative subpoena process consistent with applicable policy and law. Internal CISA policy requires that a number of safeguards be employed on systems which contain PII. Specifically, the system that manages the administrative subpoena process requires that all employees have a valid need to access and receive only the type of access required to meet their specific job duties and responsibilities. Additionally, users are required to complete security awareness training annually and training related to the administrative subpoena process.

AUDITING AND ACCOUNTABILITY

Definition: *Being accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all privacy protection requirements.*

Alignment: CISA's procedures directly align with the Auditing and Accountability FIPP because prior to issuing a subpoena, OCC and OCPO must both review the subpoena request to ensure CISA has sufficiently documented the specific vulnerability identified on the Internet-connected system or device, detailed the reason to believe that the vulnerability is related to critical infrastructure and that the device or system is not a personal device or system, and conducted a critical infrastructure security risk assessment. Additionally, in accordance with the procedures, OCPO conducted this review of requested subpoenas to verify that CISA has adhered to the procedures.

IV. Review of Agency Operations' Adherence to Procedures

Subsection (p)(9) of Section 2209 required the Privacy Officer of CISA to ensure "the operations of the Agency comply with [the internal procedures]."

OCPO assigned a team of privacy analysts to review administrative subpoenas through their entire lifecycle for this report and, to ensure the independence of the review, OCPO ensured this team of privacy analysts did not include the privacy analysts who work on administrative subpoenas daily. This review examined CISA's operational adherence to the internal procedures as they were written and attempted to identify any deficiencies, room for improvement, and failures to adhere to the internal procedures.

The process for issuing an administrative subpoena is initiated by a subpoena request from a CISA analyst. For this review, OCPO reviewed all 70 administrative subpoenas initiated in calendar year 2021, ranging from the first subpoena initiated on April 14, 2021 to the last subpoenas initiated on December 31, 2021. Since CISA's administrative subpoenas undergo internal CISA review as well as interagency coordination before issuance, subpoenas are typically not issued until some time after initiation of the process. OCPO reviewed all administrative subpoenas which were initiated in calendar year 2021, but not all of these subpoenas were issued in calendar year 2021. For this reason, this privacy review encompasses more subpoenas than are included in the "Administrative Subpoena Annual Report: Calendar Year 2021 Report to Congress" which only addresses the 47 administrative subpoenas that were initiated *and issued* prior to December 31, 2021. In this review, OCPO examined whether CISA sufficiently documented the reason to believe the vulnerability was related to critical infrastructure, as well as the reason to believe the device was not a personal device. OCPO also examined whether all reasonable steps had been taken to identify the owner and operator through other means, whether PII was deleted in a timely fashion when appropriate, and whether PII that was retained was done so with permission.

FINDINGS

In OCPO's review of the 70 administrative subpoenas requested during calendar year 2021, OCPO found that CISA's Administrative Subpoena Team adhered to the internal procedures created for the issuance of administrative subpoenas. The review verified that CISA documented each step of the process, from the initiation of the subpoena request to vetting and receiving clearance from the appropriate parties/authorities to external coordination and issuance of the subpoena. OCPO verified that each subpoena request documented sufficient reason to believe that the vulnerabilities were related to critical infrastructure and the device or system was not a personal device, and that all reasonable steps to identify the owner and operator through other means were taken. Furthermore, OCPO found that CISA employees deleted PII belonging to individuals in accordance with the procedures and in a timely manner. Further, when PII was retained, it was done so with consent from individuals.

While OCPO has concluded CISA staff adhered to the procedures, OCPO recommends process improvements for more thorough documentation of actions taken by CISA staff.

In its review, OCPO was initially unable to determine if consent was provided to retain PII beyond the 6-month time limit set out in statute and prescribed in the procedures because of incomplete documentation in CISA's case management system. As a result, OCPO relied on CISA staff to track down prior communications, such as scripts for conversations with the vulnerable entities, to confirm whether the entities were provided an opportunity to consent to their contact information being retained and the entity's response.

CISA staff stated to OCPO during its review that a large number of the initial communications with vulnerable entities occurred by telephone, and therefore consent to PII retention may not have been documented in writing. This lack of a written record made it challenging to confirm that CISA had obtained consent from individuals to retain their information; however, through interviews with CISA staff, OCPO was able to confirm that individuals consented verbally when contacted by telephone. Therefore, as long as CISA's administrative subpoena statute and procedures require that CISA seek consent to retain information no longer than 6 months, OCPO strongly recommends that CISA staff update their internal processes to ensure that written confirmation of an entity's consent or request of deletion is sought in addition to verbal consent. Further, both forms of consent should be documented in the case management system.

V. Conclusion

Consistent with subsection (p)(9) of Section 2209 of the Homeland Security Act, as amended, OCPO conducted a review of the agency's internal procedures for the administrative subpoena process and concluded that the procedures are consistent with fair information practices and that the operations of the agency comply with the procedures. This is due, in part, to OCPO's guidance during the development of the internal procedures associated with issuing administrative subpoenas and OCPO's continued involvement in the administrative subpoena process. OCPO verified that each subpoena request documented sufficient reason to believe that the vulnerabilities were related to critical infrastructure and the device or system was not a personal device, and that all reasonable steps were taken to identify the owner and operator through other means. Furthermore, OCPO found that CISA employees deleted PII belonging to vulnerable entities in accordance with the procedures and in a timely manner. Further, because subsection (p) of Section 2209 and the procedures requires that CISA destroy PII contained in subpoena responses no later than 6 months from receipt, when CISA retained PII longer than that period, it did so with consent from those entities.

OCPO recognizes that more thorough documentation and recordkeeping, specifically as it relates to documenting consent to retain an individual's PII, will further improve the administrative subpoena process. OCPO will work closely with internal stakeholders to update the internal procedures accordingly to ensure that confirmation of consent to retain PII is documented in writing and stored appropriately in the case management system.