Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
Directives System
Directive Number: 6300-01
Revision Number: N/A
Issue Date: 09/27/2023

ADMINISTRATIVE SUBPOENA FOR VULNERABILITY NOTIFICATION FUNCTION

I. General Information

A. Purpose

This Directive establishes the Cybersecurity and Infrastructure Security Agency (CISA) Administrative Subpoena for Vulnerability Notification Function and associated procedures and training, pursuant to the administrative subpoena authority granted to the CISA Director by the National Defense Authorization Act for Fiscal Year 2021, Public Law (Pub. L.) 116-283.

B. Scope of Application

This Directive applies to all employees who seek to leverage CISA's Administrative Subpoena for Vulnerability Notification Function authority and carry out the functions of the authority.

C. Exemptions

There are no exemptions to this policy.

D. Supersession

This Directive supersedes the Memorandum for Distribution Policy Statement, "Cybersecurity and Infrastructure Security Agency Administrative Subpoena Function" issued on April 2, 2021 for which applicability was formally extended to September 30, 2023.

E. Review Dates

This section is completed by SPP.

1. Last Review Date:
2. Effective Date:
3. Next Review Date:

F. **Revision Log**

This section is completed by SPP.

Revised Section Number and Title	Deleted Section Number and Title	Approved By:	Date:

II. Responsibilities

A. The **Director, CISA**:
1. Oversees the development, execution and sustainment of the Administrative Subpoena for Vulnerability Notification Function.

B. The **Executive Assistant Director (EAD), Cybersecurity Division (CSD)**:
1. Manages and executes the Administrative Subpoena authority enacted in section (p) of Section 2209 of the Homeland Security Act, as amended, and its responsibilities as delegated by the Director;
2. Issues the implementing standards and operating procedures in the "Standards and Procedures" section of this Directive;
3. Ensures collaborations, inputs in process, program management, as well as follow-on actions for vulnerable entities, by and among relevant CISA divisions and offices, including Office of the Chief Counsel (OCC), Office of Privacy, Access, Civil Liberties and Transparency (PACT), Integrated Operations Division (IOD) and CSD;
4. Manages responses to administrative subpoenas, routing information to appropriate divisions and offices within CISA when needed;
5. Executes and manages the initial notification to international entities and, where appropriate, any follow-up and long-term relationship with vulnerable entities; and
6. Oversees compliance and enforcement of requirements established for this Directive.

C. The **Chief Counsel**:
1. Evaluates administrative subpoena requests; and
2. Reviews and provides guidance on the Administrative Subpoena Annual Report and other Administrative Subpoena products as needed.

D. The **Chief of Privacy, Access, Civil Liberties, and Transparency (PACT)**:
1. Reviews administrative subpoena requests;
2. Leads the Privacy Compliance Review of the Administrative Subpoena Program on a regular and ongoing basis, to occur no less than every three years; and
3. Reviews and provides guidance on the Administrative Subpoena Annual Report and other Administrative Subpoena products, as needed.

E. The **Assistant Director, Integrated Operations Division (IOD)**:

1. Manages CISA's regional organizations; and
2. Executes and manages the initial notification to domestic entities, follow ups and maintains long-term relationships with vulnerable entities, in collaboration with other CISA capabilities that may potentially support mitigation of vulnerabilities.

III. Standards and Procedures

A. Description

1. The purpose of the CISA Administrative Subpoena for Vulnerability Notification Function is to operationalize the authority granted in Pub. L. 116-283 to issue administrative subpoenas for the production of information necessary to identify and notify vulnerable entities, as part of fulfilling the agency's cybersecurity and infrastructure security mission.

2. The Administrative Subpoena for Vulnerability Notification Function is established within CISA and composed of the following elements:
   a. Procedures for coordination of administrative subpoenas with the Department of Justice (DOJ);
   b. Internal operating procedures for execution of the function within CISA; and
   c. Required training for workforce members relevant to the function's execution.

3. Questions about this Directive may be directed to (b) (6) which is managed by the Administrative Subpoena Team within CSD. Additional materials related to authority execution including, but not limited to, the standard operating procedures are available on the CSD intranet site.

B. Implementing Standards and Procedures

1. Inter-agency coordination
   a. The issuance of administrative subpoenas is coordinated with the DOJ;
   b. Coordination occurs pursuant to the "CISA Procedures for Coordination of Administrative Subpoena with the Department of Justice" on the CSD intranet site;
   c. The Administrative Subpoena Team coordinates each subpoena request with the Federal Bureau of Investigation (FBI) in accordance with the procedures for coordination with the DOJ and follows up with FBI if the FBI fails to provide a response within 72 hours; and
   d. The EAD of CSD oversees the development and revision of this procedural agreement.

2. Operating procedures and training specifically applicable to CISA employees, contractors, detailees and agency operations
   a. The EAD of CSD oversees the development, updating and issuance of CISA's internal operating procedures and training. See "CISA Administrative

Subpoena Training" and "CISA Administrative Subpoena Operating Procedures" on the CSD intranet site.

i. CSD manages the execution of operating procedures and training, which includes reviews and approvals by OCC and PACT and tasking IOD for notification to vulnerable domestic entities;
ii. CISA employees, contractors and detailees must meet the criteria established by CSD to use the administrative subpoena capability and must undergo training for its use; and
iii. Training occurs on a regular basis for all CISA employees implementing the administrative subpoena authority, including conducting notifications.
    1) Specifics of recorded and live training are available under "CISA Administrative Subpoena Training" on the CSD intranet site.
    2) These trainings are maintained by the Administrative Subpoena Team. As trainings are developed, the Administrative Subpoena Team solicits feedback from stakeholders across the agency.

b. These procedures and training address, at a minimum:
    i. Protection of, and restriction on, dissemination of nonpublic information obtained through the subpoenas;
    ii. Restriction on the use of information obtained through subpoenas for a cybersecurity purpose;
    iii. Retention and destruction of nonpublic information obtained through subpoenas;
    iv. Process for providing notice to each party subject to a subpoena and each entity identified by information obtained under a subpoena;
    v. Processes and criteria for conducting Critical Infrastructure security risk assessments to determine whether a subpoena is necessary; and
    vi. Information to be provided to an entity at risk at the time of the vulnerability notice.

3. Subpoena Compliance Procedure
    a. If a subpoenaed entity does not comply with the administrative subpoena within a reasonable time period, or indicates no intention of complying with the subpoena, the Administrative Subpoena Team notifies OCC.
    b. If DOJ decides to initiate legal action against a noncompliant subpoena recipient to enforce the subpoena, the Administrative Subpoena Team ensures the CISA Director, or designee, is aware.

C. Compliance and Enforcement

1. Consequences for Noncompliance: CISA employee noncompliance with this Directive impacts CISA's ability to help protect vulnerable entities, which is a critical element of its mission. CISA personnel who do not comply with this Directive and the associated procedures may be subject to discipline, including remedial training, verbal or written warnings or other measures consistent with the Department of Homeland Security's Table of Penalties.

2. Compliance Procedures: The Administrative Subpoena Team provides training, as required by need-to-use, and access to the most current operating procedures on the CSD Intranet site.

3. Enforcement Methods: Enforcement methods are incorporated into the review and approval procedures and the annual audit steps conducted by PACT biannually for a privacy audit which are incorporated into the operating procedures.

IV. Authorities

A. Section 2209 of the "Homeland Security Act of 2002," as amended
B. Pub. L. 116-283, "William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021"
C. CISA Delegation DG-22-005, "Delegation of Subpoena Authority"

(b) (6)

09/27/2023

Cybersecurity and Infrastructure Security Agency

Date

Appendix A:
References

I. CSD Intranet site

Appendix B:
Definitions and Acronyms

I. Definitions

A. **Administrative Subpoena**: An administrative summons or subpoena is a judicially enforceable demand for records issued by a government authority which is authorized by some other provision of law to issue such process. The administrative subpoenas in this Directive are governed by section 2209 of the Homeland Security Act of 2002, as amended.

B. **Critical Infrastructure**: means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety or any combination of those matters.

II. Acronyms

Acronyms	
CI	Critical Infrastructure
CISA	Cybersecurity and Infrastructure Security Agency
CSD	Cybersecurity Division
DOJ	Department of Justice
EAD	Executive Assistant Director of CSD
IOD	Integrated Operations Division
FBI	Federal Bureau of Investigation
OCC	Office of the Chief Counsel
NRMC	National Risk Management Center
PACT	Office of Privacy, Access, Civil Liberties and Transparency
PII	Personally Identifiable Information
Pub. L.	Public Law
SOP	Standard Operating Procedures
TH	Threat Hunting
U.S.C.	United States Code
VM	Vulnerability Management