

## **CHIEF PRIVACY OFFICER INVESTIGATIONS**

---

### **I. Purpose**

This Instruction implements Directive 047-01, "Privacy Policy and Compliance," with regard to the Chief Privacy Officer's investigatory responsibility under 6 United States Code (U.S.C.) § 142 to address possible violations or abuse concerning the administration of DHS programs or operations affecting privacy.

### **II. Scope**

This Instruction applies throughout DHS to investigations conducted by the Chief Privacy Officer related to the collection, use, maintenance, disclosure, deletion, and destruction of Personally Identifiable Information (PII) and regarding any other activity that impacts the privacy of individuals as determined by the Chief Privacy Officer.

### **III. References**

- A. Title 5, U.S.C. Section 552a, "Records Maintained on Individuals" [The Privacy Act of 1974, as amended]
- B. Title 5, U.S.C. Appendix, "The Inspector General Act of 1978," as amended
- C. Title 6, U.S.C. Section 142, "Privacy officer"
- D. Title 12, U.S.C. § 3401 *et seq.*, "The Right to Financial Privacy Act of 1978"
- E. Title 18, U.S.C. § 2510 *et seq.*, "The Electronic Communications Privacy Act of 1986," as amended
- F. Directive 047-01, "Privacy Policy and Compliance"

G. Management Directive 11042.1, "Safeguarding Sensitive But Unclassified (For Official Use Only) Information"

H. Management Directive 0810.1, "The Office of Inspector General"

I. Memorandum of Understanding between the Chief Privacy Officer and the Inspector General, March 25, 2008 (MOU) (Attached).

## IV. Definitions

A. **Investigation**: a review, as authorized by statute, of possible violations or abuse concerning the administration of DHS programs or operations affecting privacy.

B. **Investigator**: An individual who has been authorized by the Chief Privacy Officer to conduct an investigation into possible violations or abuse concerning the administration of any DHS program or operation affecting privacy.

## V. Responsibilities

A. The **Chief Privacy Officer**

1. Coordinates activities with the Inspector General (IG), in accord with DHS Directive 047-01, the Memorandum of Understanding (MOU) between the Privacy Office and the IG, and this Instruction to avoid duplication of effort.

2. Routinely communicates with the IG regarding ongoing or possible investigations.

3. Reviews the monthly report provided by the IG, as required by Section IV of the MOU, identifying all allegations the IG has received that reflect possible violations or abuse concerning the administration of any DHS program or operation affecting privacy.

4. Coordinates, as appropriate, with the DHS Chief Intelligence Officer and the Director of National Intelligence regarding any investigation under this Instruction that involves classified national security information in the purview of DHS.

B. The **IG**:

1. Coordinates activities with the Chief Privacy Officer, in accord with DHS Directive 047-01, the MOU, and this Instruction, to avoid duplication of effort.
2. Provides a monthly report to the Chief Privacy Officer, as required by the MOU, identifying all allegations the IG has received that reflect possible violations or abuse concerning the administration of any DHS program or operation affecting privacy.

## VI. Procedures

A. Procedures for Initiating an Investigation

1. The Chief Privacy Officer refers any allegations or complaints of possible violations or abuse concerning the administration of any DHS program or operation affecting privacy to the IG as soon as possible, but no later than 30 days following the receipt of the allegation or complaint.
2. The IG determines as soon as possible, but no later than 30 days after receiving the referral from the Chief Privacy Officer, whether to investigate the allegation or complaint or refer the matter back to the Chief Privacy Officer for investigation.
3. If the IG notifies the Chief Privacy Officer that the IG does not intend to initiate an investigation, and the Chief Privacy Officer then deems an investigation to be necessary or desirable, the Chief Privacy Officer initiates an investigation.
4. The IG initiates an investigation of any matter it retains within 90 days of the decision to investigate.
5. If the IG does not initiate an investigation within 93 days of the decision to investigate, the IG notifies the Chief Privacy Officer of such.
6. If the Chief Privacy Officer receives notification that an investigation was not initiated within 93 days of the IG's decision to investigate, and the Chief Privacy Officer deems then an investigation to be necessary or desirable, the Chief Privacy Officer may initiate an investigation.

7. The Chief Privacy Officer does not initiate an investigation unless the conditions detailed in 3 or 6 above are met.

8. The Chief Privacy Officer notifies appropriate DHS officials of any Chief Privacy Officer investigations that are being conducted within their areas of responsibility.

B. Designation of Privacy Office employees to take oaths.

1. The Chief Privacy Officer may administer to, or take from any person an oath, affirmation, or affidavit, whenever necessary to perform the responsibilities of investigations of possible violations or abuse regarding privacy issues.

2. Oaths may also be administered or taken by the Deputy Chief Privacy Officer, the Director of Privacy Incidents and Inquiries, or other DHS Privacy Office official the Chief Privacy Officer authorizes in writing whenever necessary to perform an investigation.

C. Subpoena process:

1. General Policy: To the greatest extent possible, the Chief Privacy Officer seeks information, documents, reports, answers, records, accounts, papers, or other data and documentary evidence necessary to the performance of an investigation, through voluntary means, or pursuant to contractual or regulatory obligations. In the event that voluntary production is not forthcoming or possible, the Chief Privacy Officer considers issuance of a subpoena.

When circumstances dictate, the Chief Privacy Officer issues subpoenas to obtain from any person other than a federal agency, information, documents, reports, answers, records, accounts, papers, or other data and documentary evidence necessary to the performance of an investigation.

2. Subpoena Requests:

a. If the Investigator or other individual authorized by the Chief Privacy Officer determines that the issuance of a subpoena is necessary to an investigation, he or she submits a written request to the Chief Privacy Officer that reflects the need for the subpoena. If time is a critical factor, the request may be made orally and

confirmed in writing.

b. All requests for subpoenas are sent to the Chief Privacy Officer using methods required by DHS policy for transmittal of Sensitive But Unclassified (For Official Use Only) Information, and using the appropriate subpoena forms included in the appendices to this Instruction.

c. Subpoena requests include:

- i. Title and file number of the investigation;
- ii. A concise history of the investigation;
- iii. The name and address of the individual, corporation, partnership, agency, institution, or other unincorporated business whose records are sought;
- iv. The justification for the subpoena;
- v. A complete and precise description of the items to be obtained. Documents are divided into categories, and a time period related to the documents is specified (e.g. "All audit logs from January 1, 2010 to the date of this subpoena."). The use of attachments to describe the type(s) of records sought is encouraged;
- vi. Any special element of urgency, e.g., possibility of removal or destruction of records;
- vii. Whether a privilege is expected to be asserted by the subpoenaed party;
- viii. The likelihood, if any, that judicial enforcement of the subpoena will be required, or that the subpoenaed party will challenge the subpoena; and
- ix. The proposed date of service.

d. If the Chief Privacy Officer determines that a subpoena is necessary to an investigation, the Chief Privacy Officer submits the request to the Office of the General Counsel (OGC) for review

within 5 business days.

e. OGC reviews the subpoena request and any supporting documents for completeness, legal sufficiency, validity, and compliance with applicable law. OGC contacts the Chief Privacy Officer to obtain additional information as necessary.

f. After review by OGC, the Chief Privacy Officer submits the subpoena request to the Secretary for approval.<sup>1</sup>

g. If the Secretary approves the subpoena request, the Chief Privacy Officer personally approves and signs the subpoena. If a subpoena is **urgently** required, the Chief Privacy Officer may convey relevant information to OGC by telephone, and, if the Secretary approves the subpoena request, written materials may be submitted after the subpoena is issued.

3. Service of Subpoenas:

a. Service should be made as soon as possible after the subpoena is issued.

b. Subpoenas are served, by the Investigator or other individual designated by the Chief Privacy Officer, personally, via certified mail, or through counsel to the subpoenaed party as appropriate.

c. Proof of service is evidenced by a Certificate of Return of Service executed by the Investigator or other individual serving the subpoena. The Certificate of Return of Service and the original subpoena are filed in the records of the investigation. Copies of both the Certificate of Return of Service and the subpoena are sent to OGC.

d. All subpoenas include relevant forms informing the subpoenaed parties of their rights under applicable law including: Electric Communications Privacy Act (ECPA), Right to Financial Privacy Act (RFPA), and the Privacy Act. Appendix A to this

---

<sup>1</sup> By statute, if the Secretary disapproves the Chief Privacy Officer's request, or 45 days pass without the Secretary approving or disapproving the request, the Chief Privacy Officer notifies the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives as such within 30 days. 6 U.S.C. § 142(e)(2).

Instruction contains the forms required to be submitted with all subpoenas. Appendix B to this Instruction contains instructions for subpoenas covered by RFPA and the forms required for subpoenas covered by RFPA. Appendix C contains forms for subpoenas covered by ECPA.

4. Production of Records:

a. The place of appearance for the production of records is determined jointly by the Investigator and the recipient of a subpoena. If appropriate, the subpoena indicates that the records sought may be returned to the Investigator by certified mail.

b. The Investigator allows a reasonable amount of time for the production of records after service of the subpoena. In general, subpoenaed parties are given at least two weeks from the date of service to comply with a subpoena. Where an unusually short return time (less than seven days) is deemed necessary, the Investigator or Chief Privacy Officer notes the time limitation in the initial submission to OGC. The type, volume, and possibility of removal or destruction of the records is considered when setting a return date. The Chief Privacy Officer may, at his or her discretion and in writing, extend the return date for a limited period of time, upon a written request for an extension from the person upon whom the subpoena was served.

c. Absent unusual circumstances, the Investigator is entitled to original documents. The Investigator may accept copies if doing so will not adversely affect the investigation.

d. The Investigator safeguards classified documents responsive to a subpoena in a manner consistent with federal and DHS requirements regarding the handling of such documents. Classified documents are accessed and reviewed only by Privacy Office staff with appropriate clearances and a need to know.

e. If the subpoenaed party appears to have satisfied the terms of the subpoena, the Investigator prepares a memorandum attesting to this fact. The memorandum identifies the individual who produced the records, the time and place of production, and a description of the records produced. The memorandum is filed with the records of the investigation and a copy is provided to the subpoenaed party, if requested.

f. If a subpoenaed party does not comply with the terms of a Chief Privacy Officer subpoena, the Investigator notifies the Chief Privacy Officer. The Chief Privacy Officer, in consultation with OGC, determines procedures to ensure compliance. If enforcement action is desired, the Chief Privacy Officer, in consultation with OGC, coordinates such action with the Department of Justice.

5. Return of Records:

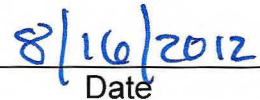
Upon completion of an investigation or when otherwise appropriate, the Investigator returns original documents to the subpoena recipient or records custodian, unless the Privacy Office has written authorization from the subpoenaed party that such records are no longer needed and do not need to be returned. The Investigator obtains a receipt for all returned documents.

## VII. Questions

Address any questions or concerns regarding this Instruction to the DHS Privacy Office or to the relevant Component Privacy Officer or PPOC.

  
Jonathan R. Cantor

Acting Chief Privacy Officer

  
Date