Department of Homeland Security
DHS Directives System
Instruction Number: 047-01-006
Revision Number: 00
Issue Date: DECEMBER 4, 2017

PRIVACY INCIDENT RESPONSIBILITIES AND BREACH RESPONSE TEAM

I. Purpose

This Instruction implements the Department of Homeland Security (DHS) Directive 047-01, "Privacy Policy and Compliance," and establishes DHS policy, responsibilities, and requirements for responding to all incidents involving personally identifiable information (PII)[1] contained in DHS information (i.e., "privacy incident"/"breach").[2] This instruction also establishes the requirement for the Chief Privacy Officer to convene and lead a Breach Response Team (BRT) when a "major incident" that includes PII has occurred[3] or at the discretion of the Chief Privacy Office.

II. Scope

This Instruction applies to DHS employees, including the Chief Privacy Officer, and offices, in handling and responding to privacy incidents.

[1] DHS defines PII as "any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the U.S., or employee or contractor to the Department." DHS Handbook for Safeguarding Sensitive Personally Identifiable Information.

[2] DHS defines a "privacy incident" as the following: "The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than the authorized user accesses or potentially accesses [PII] or (2) an authorized user accesses or potentially accesses [PII] for an unauthorized purpose. The term encompasses both suspected and confirmed incidents involving PII, whether intentional or inadvertent, which raises a reasonable risk of harm." This new definition for "privacy incident" for the Department comports with the Office of Management and Budget's (OMB) definition of a "breach" in OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of PII" (Jan. 3, 2017). The term "privacy incident" will be used synonymously with the term "breach" for this Instruction. The term "privacy incident" does not include or pertain to doxxing, which is described in DHS Policy Directive 121-07, "Standard Procedures When Restricted Personal Information (also known as Sensitive Personally Identifiable Information) is Posted on the Internet and/or Social Media (Doxxing)."

[3] A breach constitutes a "major incident" when it involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. An unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to 100,000 or more individuals' PII constitutes a "major incident." See OMB M-18-02 and subsequent OMB Guidance. The Chief Privacy Officer, in coordination with the Chief Information Officer (CIO) and Chief Information Security Officer (CISO), will first determine whether the privacy incident is considered a "major incident" that involves PII.

III. Authorities

A. Title 5, United States Code (U.S.C.), Section 552a, “Records Maintained on Individuals” [The Privacy Act of 1974, as amended]

B. Title 6, U.S.C., Section 142, “Privacy Officer”

C. Title 44, U.S.C., Chapter 35, Subchapter II, “Information Security” [The Federal Information Security Modernization Act of 2014, as amended (FISMA)]

D. Office of Management and Budget (OMB) Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016)

E. OMB Memorandum 16-24, Role and Designation of Senior Agency Officials for Privacy (September 15, 2016)

F. OMB Memorandum 17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017)

G. OMB Memorandum 18-02, Fiscal Year 2017 - 2018 Guidance On Federal Information Security And Privacy Management Requirements (October 16, 2017), and subsequent OMB Fiscal Year Guidance on Federal Information Security and Privacy Management Requirements

H. DHS Delegation 13001, “Delegation to the Chief Privacy Officer”

I. DHS Delegation 04000, “Delegation for Information Technology”

J. DHS Policy Directive 140-07, “DHS Privacy Incident Handling Guidance (PIHG)”

K. DHS Instruction 047-01-005, “Component Privacy Officer”

L. DHS 4300A, “Sensitive Systems Policy,” DHS 4300A Sensitive Systems Policy Handbook, Attachment F, “Incident Response”

IV. General Responsibilities

When a privacy incident is first identified and reported into the Department's Enterprise Security Operations Center (DHS ESOC) portal, the DHS ESOC notifies the Chief Privacy Officer or DHS Privacy Office (PRIV) staff of the incident.[4] Concurrently, the DHS ESOC will also notify the Component Privacy Office staff and Component ESOC, as well as DHS Office of the Chief Security Officer (OCSO), Threat Management Operations, immediately following receipt of an incident.

All other incidents[5] are managed and addressed by the Office of Chief Information Officer (OCIO) pursuant to DHS's 4300A, "Sensitive Systems Policy."

A. When first made aware of a privacy incident, the ***DHS Chief Privacy Officer***:

1. Serves as the senior DHS official responsible for oversight of privacy incident management.

2. Evaluates the sensitivity of the PII involved in the privacy incident and assesses the risk of harm to individuals potentially affected by the privacy incident. Determines whether the Department's response can be conducted at the direction of the Component Privacy Officer or whether to convene the BRT.[6]

3. The Chief Privacy Officer shall consult with the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) to determine whether a privacy incident constitutes a "major incident" and if so, will convene the BRT within 72 hours of that consultation and determination. At a minimum, the BRT is convened when a privacy incident constitutes a "major incident", as defined in OMB M-18-02, and subsequent guidance issued by OMB.

4. Reports, with coordination of the members of the BRT, all major incidents that involved a privacy incident to Congress, as required by FISMA.[7]

---

[4] See DHS 4300A Sensitive Systems Handbook, Attachment F, Incident Response.

[5] An "incident" is defined as "an occurrence that, (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies." 44 U.S.C. § 3552(b)(2).

[6] The term BRT is used synonymously with the term Privacy Incident Response Team (PIRT) and identified as such as part of DHS's Privacy Incident Handling Guidance (PIHG).

[7] *See* 44 U.S.C. § 3554(b)(7).

5. Leads and manages the BRT once convened.

6. Works with Component Privacy Officers to ensure incidents are properly reported, investigated, and mitigated.

7. Gathers, analyzes, and preserves any and all evidence necessary to support an investigation of a privacy incident, if necessary, and in accordance with section 222 of the Homeland Security Act of 2002.

8. Refers all privacy incidents that may contain indicia of fraud, waste, and abuse to the Office of Inspector General.

9. Determines whether escalation is needed to Department leadership.

10. Coordinates with the DHS Office of Public Affairs (OPA) to provide reasonable advance internal notice to DHS senior officials by email or voicemail of a notification decision before notification.

B. The ***DHS Chief Information Officer (DHS CIO)***:

1. Provides management direction for the DHS ESOC and overall direction for the Component Security Operations Centers (Component SOC(s)), and ensures oversight and compliance with DHS policy regarding privacy incident responses.

2. Identifies, directs, and conducts technical remediation and forensic capabilities that exist within the Department, determines which offices are responsible for maintaining those capabilities, and provides technical support to respond to a privacy incident.

3. Evaluates the implementation and effectiveness of security safeguards, when assessing the likelihood of access and use of PII potentially compromised by a privacy incident.

4. Is a member of the BRT when convened.

C. The ***DHS Chief Information Security Officer (DHS CISO)***:

1. Oversees the DHS ESOC, providing security oversight and information assurance for all DHS information systems, including assessing the risk and magnitude of harm to such systems resulting from a privacy incident.

2. Briefs the DHS CIO and other senior management officials on significant and major incidents, providing the status of ongoing investigations and the outcomes of completed investigations.

3. Ensures that incidents are reported to US-CERT in accordance with federal regulations and approves such reports prior to their release to external government entities.

4. Is a member of the BRT when convened.

D. The ***DHS Chief Security Officer (DHS CSO)***:

1. Evaluates the privacy incident for indicators of security abnormalities and coordinates potential nefarious findings with internal and external security and law enforcement elements.

2. Conducts an Operations Security (OPSEC) review of the incident and recommends measures to strengthen the Department's ability to prevent inadvertent disclosure of information.

3. Is a member of the BRT when convened.

E. The ***Component Privacy Officers***:

1. Receive, evaluate, document, and report privacy incidents that impact Components and updates the enterprise incident database.

2. Consult with the Component Chief Information Officer and work with the Component SOC to mitigate the privacy incident.

3. Handle the investigation, notification, and mitigation for all privacy incidents; however, if the BRT is convened, the Chief Privacy Officer is responsible for leading the management of the incident, including making recommendations to the Secretary regarding notification to affected individuals. Notification must be consistent with the needs of law enforcement, national security, and any measures necessary for DHS to determine the scope of the incident, and if applicable, restore the reasonable integrity of the data system.

4. Are members of the BRT when convened only if they represent the affected Component.

F. The ***Component Heads***:

1. Consult with the Component Privacy Officer/Privacy Point of Contact (PPOC) regarding privacy issues affecting the Component.

2. Provide advice, and expertise to the BRT and/or the Component Privacy Officer/PPOC as needed to assist with the investigation, mitigation, and remediation of a privacy incident.

G. The ***Component Chief Information Officers***:

1. Work with a Component SOC and Component Privacy Officer on handling the privacy incident.

2. Consult the DHS CIO of any issues arising from any privacy incident that affects infrastructure protection or vulnerabilities.

3. Ensure any incident is reported to the DHS ESOC within established reporting time requirements.

H. The ***DHS Enterprise Security Operations Center (DHS ESOC)***:

1. Serves as a central repository and coordination point for privacy incidents within DHS.

2. Reviews and evaluates the privacy incident report for sufficiency, transmits such report to US-CERT within one hour of receipt from the Component Privacy Officer or Component SOC, and provides technical assistance as needed.

3. In cases involving PII, seeks PRIV approval to close any privacy incident.

I. The ***Component Security Operations Centers (Component SOC(s))***:

1. Consult with the Component Privacy Officer and Component CISO regarding privacy issues affecting the security of information.

2. Assist the Component Privacy Officer in preparing the privacy incident report.

3. Investigate and remediate aspects of the incident that impact computer security and provide advice and assistance as needed.

J. The ***United States Computer Emergency Readiness Team (US-CERT)*** serves as the designated central reporting organization and repository within the Federal Government for incidents, communicates and coordinates with DHS ESOC to obtain updates regarding the privacy incident, if necessary, and is responsible for notifying OMB within one hour of the privacy incident, if deemed a "major incident."

Additional information on the responsibilities of these individuals stated above and others[8] are provided in more detail in DHS Policy Directive 140-07, "Privacy Incident Handling Guidance."

V. Breach Response Team

When a "major incident" that includes PII, as described by OMB M-18-02 and subsequent guidance issued by OMB, has occurred and is identified as such, the Breach Response Team (BRT) shall be convened, and led by the Chief Privacy Officer, within 72 hours of first being notified of the privacy incident, or at a time when additional facts are presented that move the Chief Privacy Officer to convene the BRT.

A. The ***DHS Chief Privacy Officer*** coordinates with Department and Component officials responsible for handling the privacy incident; reports to the DHS Secretary and/or the DHS Deputy Secretary or the Secretary's designee; and leads the BRT to address the diverse range of legal, operational, technical, and policy challenges that could arise as a result of the major incident or other serious privacy incident or breach.

B. The ***Breach Response Team (BRT)*** supports the Chief Privacy Officer. In addition to the Chief Privacy Officer, the BRT may be comprised of representatives from the following offices [9] as warranted by circumstances of the incident:

- The DHS Deputy Secretary;
- The DHS CIO;
- The DHS CISO;
- The DHS CSO;

[8] This includes the DHS Office of Inspector General, the DHS Office of the General Counsel and Component Office of the Chief Counsel, the DHS Public Affairs Office and Public Affairs Office for the Component, the DHS Legislative Affairs Office and Legislative Affairs Office for the Component, the DHS Office of Partnership and Engagement, the DHS Management Office and Management Staff for the Component, the Chief Human Capital Officer and Component Human Capital Officers, the DHS Chief Security Officer and Component Security Officers, the DHS and Component Chief Financial Officers, the DHS Deputy Secretary, and DHS Secretary.

[9] Each individual listed in the following list may designate a senior level executive official to represent that office on his or her behalf.

- The DHS Chief Financial Officer (CFO);
- The DHS General Counsel;
- The DHS Inspector General;
- The DHS Under Secretary for Management;
- The DHS Assistant Secretary for the Office of Countering Weapons of Mass Destruction;
- The DHS Assistant Secretary for Intergovernmental Affairs;
- The DHS Assistant Secretary for Public Affairs;
- The DHS Assistant Secretary for Legislative Affairs;
- The DHS Privacy Office, Director of Privacy Incidents;

- Affected Component:
    - Component IT Security Entity (e.g., Component Information Systems Security Manager (ISSM), Computer Security Incident Response Center (CSIRC), Component SOC);
    - Component Privacy Officer or PPOC for the Component in which the incident occurred;
    - Program Manager (PM) for the program in which the incident occurred;
    - Component CIO;
    - Component Office of the Chief Counsel (OCC);
    - Communications office representative for the Component;
    - Legislative and/or inter-governmental affairs office for the Component;
    - Management Office for the Component;
    - Component CFO; and

- Additional subject matter experts may be added by the Chief Privacy Officer.[10]

C. The BRT[11] determines the appropriate course of action with respect to any privacy incident investigation, remedy options, resource allocation, risk mitigation, and interagency engagement. The Chief Privacy Officer provides recommendations to the Secretary regarding the issuance of notification to affected individuals, including the timeliness, contents, means, sources, and general appropriateness of notification; and elevates matters to the Deputy Secretary if the BRT requires additional guidance or to resolve conflicts.

VI. BRT Roles and Responsibilities

When handling an incident, DHS personnel must respond in a manner that protects PII that is the responsibility of DHS. This obligation applies to oral, paper, and electronic formats. DHS Components and personnel must understand and adhere to all relevant federal laws, regulations, and directives, and to Departmental directives and guidance. The BRT roles and responsibilities include:

A. Understand the Privacy Incident handling process and procedures.

B. Provide advice and assistance to the Component Privacy Officers/PPOCs and DHS PRIV, Director of Privacy Incidents, regarding investigation, notification, and mitigation of privacy incidents as needed.

C. Coordinate with external entities such as law enforcement during the investigation, notification, or mitigation stages as needed.

D. Provide recommendations regarding the issuance of notification to affected individuals and a press release.

E. Review Departmental implementation of privacy handling guidance at least annually or whenever there is a material change in Departmental practices in light of the mandates of the Privacy Act.

[10] For instance, the Chief Privacy Officer may need to consult with the following personnel: budget and procurement personnel, human resources personnel, law enforcement personnel, physical security personnel, and other Department personnel who may be necessary according to specific agency missions, authorities, circumstances, and identified risks.

[11] The BRT may convene in the form of a Senior Leadership Group (SLG) meeting. The SLG provides for rapid action, a senior leader forum to facilitate situational awareness, decision making, and a unity of effort. The intent of the SLG is for the Secretary to obtain quick, critical advice to address incidents, including privacy incidents and breaches, to communicate decisions and guidance; and at the headquarters level, facilitate the integration and coordination of intra-departmental operations, missions, activities, and programs. The Department's Office of Operations Coordination (OPS) facilitates the SLG meetings.

F. Convene with the Chief Privacy Officer and/or PRIV to review lessons learned after responding to a privacy incident that was reported to Congress.

G. Convene with the Chief Privacy Officer annually to conduct Tabletop Exercises to further refine and validate the breach response plan (i.e., Privacy Incident Handling Guidance) and identify potential weaknesses in the Department's response plan.

VII. Reporting and Tracking Requirements

Major Incidents:

A. Consistent with the Department's incident policies and US-CERT notification guidelines,[12] the DHS ESOC notifies US-CERT of a privacy incident within one hour of receiving the report from the Component SOC.

B. Any "major incident" is reported to US-CERT within one hour of determining an incident to be "major". Additionally, the DHS ESOC updates US-CERT within one hour of determining that an already-reported incident has been determined to be major.

C. If the Department determines a "major incident" has occurred, US-CERT is required to notify OMB within one hour of US-CERT being alerted.

D. A Department official notifies the appropriate Congressional Committees pursuant to FISMA no later than seven days after the date on which there is a reasonable basis to conclude that a "major incident" has occurred. The Chief Privacy Officer reports, with coordination of the members of the BRT, all major incidents that involved a breach to Congress. All other major incidents are reported by the DHS CIO. In addition, the Chief Privacy Officer shall supplement the initial seven-day notification to Congress with a report no later than 30 days after the Department discovers the privacy incident with additional information. This notification is consistent with FISMA and OMB guidance on reporting the breach to Congress.

[12] The DHS ESOC is also responsible for providing an annual report during the fiscal year to the Chief Privacy Officer detailing the status of each breach reported to the principal SOC. The Chief Privacy Officer shall review the report and validate that the report accurately reflects the status of each breach.

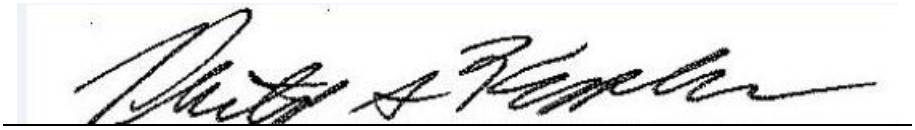
E. FISMA requires the Department, led by the DHS CIO, to submit an annual report to Congress on the adequacy and effectiveness of information security policies, procedures, and practices, which includes a description of each major incident that involved a breach of PII.[13] In addition, the DHS CIO is required to include in its annual report descriptions of the Department's implementation of the requirements in OMB M-17-12. The OCIO is responsible for submitting this report to Congress.[14]

All other incidents:

A. All other reporting and tracking requirements regarding minor privacy incidents may be found in DHS's "Privacy Incident Handling Guidance." All other reporting and tracking requirements regarding non-privacy incidents may be found in DHS's 4300A, "Sensitive Systems Policy."

VIII. Questions

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



Philip S. Kaplan
Chief Privacy Officer

12/4/2017
Date

[13] *See* 44 U.S.C. § 3554(c).

[14] Office of Management and Budget (OMB) Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016)