



# Privacy Incident Handling Guidance

DHS Instruction Guide 047-01-008

Published by the DHS Privacy Office

December 4, 2017



Homeland  
Security

# Table of Contents

<b>Introduction.....</b>	<b>3</b>
<b>Scope .....</b>	<b>6</b>
<b>Authorities .....</b>	<b>7</b>
Federal Statutes.....	5
OMB/Government-wide Regulations .....	7
DHS Policy .....	6
<b>Responding to Privacy Incidents.....</b>	<b>8</b>
Overview.....	8
Roles and Responsibilities .....	8
Privacy Incident Identification .....	13
Privacy Incident Reporting: Intake and Opening a SEN.....	14
Privacy Incident Assessment: PII Determination .....	15
Privacy Incident Assessment: US-CERT—DHS SOC and Official Notice to DHS Officials .....	17
Privacy Incident Reporting: Distinguishing between Minor and Major Incidents.....	18
Congressional Notification .....	19
Convening the Breach Response Team .....	19
Assessing the Risk of Harm to Individuals (Risk Assessment) .....	20
Mitigation.....	27
Notification for a Privacy Incident .....	28
Closure .....	34
Lessons Learned .....	35
<b>Conclusion .....</b>	<b>36</b>
<b>Appendices .....</b>	<b>37</b>
Privacy Incident Contact Information .....	38
DHS Privacy Incident Process: Minor and Major Privacy Incidents .....	39
DHS Headquarters Incident Intake Form.....	49
Definitions .....	50
Acronyms.....	53

# Introduction

In its mission to secure the homeland, the Department of Homeland Security (DHS or Department) collects personal information, known also as Personally Identifiable Information (PII). This information can come from U.S. citizens, lawful permanent residents, visitors, and non-immigrant aliens. DHS has a duty to safeguard all information in its possession, and to prevent the compromise of that PII in order to maintain the public's trust in the Department.

The Privacy Incident Handling Guidance (PIHG) supports the Department's effort to safeguard information by informing its Components, employees, senior officials, and contractors of their obligation to protect PII.

The PIHG establishes DHS policy for responding to "privacy incidents"<sup>1</sup> by providing procedures to follow upon the detection or discovery of a suspected or confirmed incident involving PII.

For purposes of this guidance, 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 United States citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department".<sup>2</sup>

**Sensitive PII** as "personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual." Examples of Sensitive PII include, but are not limited to:

- Social Security numbers (SSN),
- drivers license or state identification numbers,
- passport numbers,
- Alien Registration numbers,
- financial account numbers,
- biometric identifiers, and

- 
1. 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 definition 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 Personally Identifiable Information." (Jan. 3, 2017). The term "privacy incident" can be used synonymously with the term "breach." The DHS Privacy Incident Handling Guidance is being updated based in part on OMB Memorandum M-17-12. According to OMB, a breach is a type of incident. OMB M-17-12 further defines the appropriate reporting, handling, and notification procedures in the event a breach occurs. This guidance uses "privacy incident" and "breach" interchangeably. An incident is "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." See 44 U.S.C. § 3552(b)(2).
  2. This definition comports with DHS Sensitive Systems Policy Directive 4300A, Version 13.1, July 27, 2017, and DHS 4300A Sensitive Systems Handbook, Version 12.0, November 15, 2015.

- Other data, when combined, may also constitute Sensitive PII, such as:
  - citizenship or immigration status,
  - medical information,
  - salary,
  - ethnic or religious affiliation,
  - personal email address, address, and phone
  - account passwords,
  - date of birth,
  - criminal history, or
  - mother’s maiden name.<sup>3</sup>

As an employee, appointee, detailee, intern, contractor, grantee, or consultant (hereafter, DHS personnel), you have an obligation to report suspected or confirmed privacy incidents in a timely manner. By reporting a privacy incident in a timely manner, DHS personnel can initiate the privacy incident response process, which is required by federal law and policy.

The PIHG is an instructional “roadmap” for responding to privacy incidents, addressing reporting to resolution of an incident, as well as developing lessons learned. This guidance describes the roles and responsibilities of DHS personnel, including employees, supervisors, Component Privacy Officers/Privacy Points of Contact (PPOCs) as well as the responsible Security Operations Center (SOC). All have a critical role at the outset in establishing facts that will be needed, not only to contain the privacy incident, but also to identify appropriate mitigations and lessons learned.

Privacy incidents, whether accidental or malicious, can pose specific risks to individuals, because there is an increasing recognition that personal information such as Social Security numbers, financial account information, health information, and biometric data, is valuable and can be reverse engineered with a potential for great public harm. Therefore, it is crucial that DHS personnel be able to identify and report a suspected or confirmed privacy incident. Taking immediate action to report a suspected or confirmed privacy incident is the first step in containing, mitigating, and remediating a privacy incident.

3. See DHS Privacy Policy Directive 140-10, “Handbook for Safeguarding Sensitive Personally Identifiable Information,” for more information about policies and procedures for handling Sensitive PII.

What is PII?
PII includes your name and your work email, address, and phone
What is Sensitive PII?
STAND ALONE
• Social Security numbers
• Driver's license or state ID numbers
• Passport numbers
• Alien Registration numbers
• Financial account numbers
• Biometric identifiers
IN COMBINATION
• Citizenship or immigration status
• Medical information
• Ethnic or religious affiliation
• Personal email, address, and phone
• Account passwords
• Last 4 digits of the SSN
• Date of birth
• Criminal History
• Mother’s maiden name

OMB Memorandum M-16-04 crystalizes the challenges facing the Federal Government with respect to privacy and where efforts should be targeted:

*The unprecedented volume of PII maintained by the Federal Government today, coupled with the rapidly evolving threat and risk landscape, necessitate that agencies take an aggressive approach to protecting Federal information resources. As a result, the Federal Government has invested significant resources and efforts to ensure that protecting information resources remains a top priority.<sup>4</sup> These efforts have included strengthening government-wide processes for developing, implementing, and institutionalizing best practices;<sup>5</sup> leveraging cutting-edge technologies;<sup>6</sup> and proposing a significant budget to start the overhaul of antiquated IT systems.<sup>7</sup>*

- 
4. See OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government* (Oct. 30, 2015), available at <https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf>
  5. See *id.*
  6. *Laying the Foundation for a More Secure, Modern Government*, White House, available at <https://obamawhitehouse.archives.gov/blog/2016/10/26/laying-foundation-more-secure-modern-government> (accessed Oct. 3, 2017).
  7. See *id.* (stating that the proposed IT Modernization Fund is intended to kick-start an overhaul of antiquated Federal Government Information Technology (IT) systems and transition to new, more secure, efficient, and modern systems).

# Scope

The PIHG applies to all DHS personnel using, or with access to, DHS information and information systems in an **unclassified** environment<sup>8</sup> in any format (e.g., paper, electronic). Although most incidents involve information technology, a privacy incident may also involve oral, paper, electronic, and physical security considerations that may cause the compromise of PII.

Detailed guidance on privacy incidents can be found in the following guidance documents:

- Privacy incident handling of federal information in a classified environment, refer to *DHS 4300A Sensitive Systems Handbook, Attachment F to Handbook Version 11.0, Incident Response, Version 11.0, April 24, 2015*.
- Privacy incident handling that impacts the security of an information technology (IT) system, refer to the *DHS 4300B, National Security Systems (NSS) Policy*.
- Incident identification, classification, handling, reporting, and adherence to FISMA requirements, refer to *DHS Component User's Guide for the Department of Homeland Security Operations Center Enterprise Incident Database (ECOP) Portal*.

---

8. See DHS Administrative Security Program Instruction 121-01-011.

# Authorities

DHS has an obligation to safeguard PII and implement procedures for handling both privacy and computer security incidents. This obligation is defined in numerous federal statutes, regulations, and directives, including:

## Federal Statutes

- Title 5, United States Code (U.S.C.), Section 552a, "Records Maintained on Individuals" [The Privacy Act of 1974, as amended]
- Title 6, U.S.C., Section 142, "Privacy Officer"
- Title 44, U.S.C., Chapter 35, Subchapter II, "Information Security" [The Federal Information Security Modernization Act of 2014, as amended (FISMA)]

## OMB/Government-wide Regulations and Guidelines

- Office of Management and Budget (OMB) Circular No. A-130, Management of Federal Information Resources (updated July 28, 2016)
- OMB Memorandum 16-24, Role and Designation of Senior Agency Officials for Privacy (September 15, 2016)
- OMB Memorandum 18-02, Fiscal Year 2016 - 2017 Guidance On Federal Information Security And Privacy Management Requirements (October 16, 2017)
- OMB Memorandum 17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017)

## DHS Policy

- DHS Delegation 13001, "Delegation to the Chief Privacy Officer"
- DHS Delegation 04000, "Delegation for Information Technology"
- DHS Directive 047-01, "Privacy Policy and Compliance"
- DHS Instruction 047-01-005, "Component Privacy Officer"
- DHS Instruction 047-01-006, " Privacy Incident Response and Breach Response Team"
- DHS Privacy Policy Directive 140-10, "Handbook for Safeguarding Sensitive Personally Identifiable Information"
- DHS 4300A, "Sensitive Systems Policy," DHS 4300A Sensitive Systems Policy Handbook, Attachment F, "Incident Response"
- DHS 4300 B, "National Security Systems (NSS) Policy"
- DHS Management Directive 026-04, Protection of Human Subjects
- DHS Management Directive 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information
- DHS Management Directive 11056.1, Sensitive Security Information

# Responding to Privacy Incidents Involving PII

## Overview

When DHS personnel discover a suspected or confirmed privacy incident, there are a series of actions and activities that must occur to appropriately report, investigate, respond, and mitigate the privacy incident.<sup>9</sup>

A quick and effective response is critical to efforts to prevent or minimize any consequent harm. An effective response necessitates disclosure of information regarding the incident to those individuals affected by it, as well as to persons and entities in a position to cooperate, either by playing a role in preventing or minimizing harms from the breach or assisting in notification to affected individuals.

DHS must be able to respond in a manner that not only protects its own information but also helps to protect the information of others who might be affected by the incident. In order to fulfill this mandate, privacy incident reporting must be given high priority within DHS, and strict reporting standards and timelines must be followed.

Incident handling for the various stages must be performed in the order of priority as warranted by the circumstances. When handling privacy incidents, please keep the following in mind:

- Use and reference the PIHG. The distinct roles and responsibilities of DHS personnel and offices, as well as the activities and procedures described herein, are required upon the detection or discovery of a suspected or confirmed incident involving PII to effectively contain, mitigate, and resolve the privacy incident.
- Keep in mind the order of the incident handling stages may differ from one incident to another.
- Use your best judgment in executing incident handling responsibilities.
- Act on an informed basis in good faith and in the best interests of DHS and individuals affected by the privacy incident.
- Refer to the DHS Concept of Operations (CONOPS) if a privacy incident also impacts the security of an IT system. In this situation, both the PIHG and the CONOPS would govern incident handling because the incident would constitute both a privacy incident and a computer security incident.
- Internal notifications and access must be limited to those who have a legitimate need to know.

## Roles and Responsibilities

When handling an incident, DHS personnel must respond in a manner that protects PII maintained by DHS or stored on DHS systems. This obligation applies to oral, paper, and electronic formats. DHS Components and personnel must be cognizant and adhere to all relevant federal laws, regulations, and directives, and to Departmental guidance, in the performance of their roles and responsibilities in incidents involving PII. Once a privacy incident is reported, the manner in which the incident is

---

9. See footnote 1, *supra*, for the definition of "privacy incident."

handled impacts how effectively the privacy incident is contained, mitigated, and resolved. Below are the privacy incident handling responsibilities for the following individuals.

### DHS Chief Privacy Officer

- Serves as the senior DHS official responsible for oversight of privacy incident management.
- Responsible for determining whether the Department's response can be conducted at the direction of the Component Privacy Officer/PPOC or whether the Chief Privacy Officer convenes the Breach Response Team (BRT). The Chief Privacy Officer may choose not to convene the BRT if the response can be conducted at the Component level. At a minimum, the BRT is convened when a privacy incident constitutes a "major incident," as defined in OMB M-18-02<sup>10</sup> and subsequent OMB Guidance.
- Leads and manages the BRT once convened.
- Refers all privacy incidents that may contain indicia of fraud, waste, and abuse to the Office of Inspector General.
- Evaluates the sensitivity of the PII involved in the privacy incident and assesses the risk of harm to individuals affected by the privacy incident.
- Directs BRT or Component Privacy Officer/PPOC to gather, analyze, and preserve any and all evidence necessary to support an investigation of a privacy incident, in accordance with Section 222 of the Homeland Security Act of 2002.
- Consults with the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) to determine whether a privacy incident constitutes a major incident pursuant to OMB M-18-02, and subsequent OMB Guidance, which may trigger Congressional reporting requirements under the FISMA.<sup>11</sup>
- Provides recommendations for notification options to the Secretary after consultation with the BRT regarding a major privacy incident.
- Elevates issues to the Deputy Secretary if the BRT requires additional guidance or conflict resolution.

### DHS Breach Response Team

- Supports the DHS Chief Privacy Officer to identify appropriate course of action with respect to any major privacy incident investigation, remedy options, resource allocation, notification to impacted individuals, risk mitigation, interagency engagement, and the timeliness, content, means, sources, and general appropriateness of other external notification. After consultation with the BRT, the DHS Chief Privacy Officer provides recommendations to the Secretary regarding the issuance of notification to affected individuals, including timeliness, contents, means, sources, and general appropriateness of notifications; and elevates matters to the Deputy Secretary if the BRT requires additional guidance or to resolve conflicts.

---

10. 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 DHS Chief Privacy Officer, in coordination with the CIO and CISO, will first determine whether the privacy incident is considered a "major" incident that involves PII.

11. See 44 U.S.C. § 3554(b)(7).

- The BRT includes, at a minimum, the following officials or their representatives:<sup>12</sup>
  - DHS Under Secretary for Management
  - DHS CIO
  - DHS CISO
  - DHS General Counsel
  - Assistant Secretary for Public Affairs
  - Assistant Secretary for Legislative Affairs
  - Affected Component offices impacted by the privacy incident
- As necessary, depending on the type of incident, the DHS Chief Privacy Officer may request additional subject matter experts to join and assist the BRT. For example, if the privacy incident involves financial information, the DHS Chief Privacy Officer may request the DHS Chief Financial Officer to join the BRT.
- The BRT is supported by the DHS Privacy Office's Director of Incidents and the Component Privacy Officers/PPOCs.

#### DHS Privacy Office, Director of Privacy Incidents

- Consults with the Component Privacy Officer/PPOC on incident assessment.
- Determines if incident requires consultation and notice to other components and DHS stakeholders.
- Responsible for working with Component Privacy Officer/PPOCs to ensure incidents are properly reported, investigated, and mitigated. In addition, all privacy incidents are reviewed for accuracy and completeness.
- Obtains from the Component Privacy Officer/PPOC information identifying the system of records notice (SORN), Privacy Impact Assessment (PIA), and/or other existing compliance documents that may apply to the compromised PII.
- Oversees, with the Component Privacy Officer/PPOC, operational activities of the BRT.
- Coordinates, as required, with the DHS Chief Privacy Officer and Office of Public Affairs to provide *reasonable advance internal notice* to DHS senior officials by email or voicemail of a notification decision before external notification.
- Participates on the BRT when convened.
- Reviews incident closure request with Component Privacy Officer/PPOC.
- Notifies DHS SOC when an incident is closed, or if the incident will remain open for review or further incident handling.

#### DHS Chief Information Officer (DHS CIO)

- Provides management direction for the DHS SOC and overall direction for the responsible SOCs, and ensures oversight and compliance with DHS policy regarding privacy incident responses.
- Identifies, directs, and conducts technical remediation and forensic capabilities that exist within the Department and which offices are responsible for maintaining those

---

12. 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, 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 SLG meetings.

capabilities, which provides technical support to respond to a privacy incident.

- Is a member of the BRT when convened.
- Evaluates the implementation and effectiveness of security safeguards when assessing the likelihood of access and use of PII compromised by a privacy incident.

#### DHS Chief Information Security Officer (DHS CISO)

- Oversees the DHS SOC, 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.
- Briefs the CIO and other senior management officials on significant and major privacy incidents that impact availability, confidentiality, and integrity of network/system assets, provides the status of ongoing investigations, and the outcomes of completed investigations.
- Is a member of the BRT when convened.
- Ensures that incidents are reported to US-CERT in accordance with federal regulations and guidance, and approves of such reports prior to their release to external government entities.

#### DHS Security Operations Center (DHS SOC)

- Serves as a central repository and coordination point for privacy incidents within DHS.
- 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/PPOC or responsible SOC, and provides technical assistance as needed.
- Seeks approval to close any privacy incident from PRIV in cases involving PII.

#### Component Heads

- Provide necessary resources or assistance to facilitate the handling of any privacy incident that affects its Component.

#### Component Privacy Officers/PPOCs

- Receive, evaluate, document, and report privacy incidents that impact Components and updating the enterprise incident database.
- Oversee, with the DHS Privacy Office's Director of Privacy Incidents, operational activities of the BRT.
- Consult with the Component Chief Information Officer and work with their respective Component Security Operations Center (SOC) to mitigate the privacy incident.
- Provide incident closure request for DHS Privacy Office's Director of Privacy Incidents review.
- Are members of the BRT when convened only if they represent the affected component.
- Handle the investigation, notification, and mitigation for all minor privacy incidents. However, if the BRT is convened, the Chief Privacy Officer is responsible for leading the management of the incident, including providing external notification to affected individuals of the party. 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 to the data of the compromised system.

### Component Chief Information Officer

- Responsible for establishing and working with a responsible SOC, working with the Component Privacy Officer/PPOC on handling the privacy incident, consulting the DHS CIO of any issues arising from any privacy incident that affects infrastructure protection or vulnerabilities, and ensuring that any incident is reported to the DHS SOC within established reporting time requirements.

### Responsible Security Operations Center (SOC)

- Recognize privacy incidents and understand the privacy incident reporting process and procedures.
- Consults with the Component Privacy Officer/PPOC regarding privacy issues affecting the security of information, assists the Component Privacy Officer/PPOC in preparing the Privacy Incident Report, investigates and remediates aspects of the incident that impact computer security, and provides advice and assistance as needed.
- Provide advice, expertise, and assistance to BRT as needed.

### DHS Personnel

- Complete the mandatory annual online Privacy Awareness Training and Education.
- Recognize and report privacy incidents.
- Inform a supervisor, responsible SOC, or the Component Privacy Officer/PPOC of the detection or discovery of suspected or confirmed privacy incident.
- **Contractors and subcontractors** are required to follow Homeland Security Acquisition Regulation (HSAR) provisions when handling Sensitive PII. Moreover, contractors and subcontractors must cooperate with DHS and exchange information as necessary in order to effectively report and manage a suspected or confirmed privacy incident, including risk assessment, mitigation, and notification in the case of a major privacy incident.
- **Grant recipients and grantees** must have procedures in place to respond to a privacy incident and notify the DHS in the event of a privacy incident. The procedures should promote cooperation and the free exchange of information with the Department grant officials, as needed, to properly escalate, refer, and respond to a privacy incident.

### DHS Supervisors and Program Managers

- Ensure compliance with federal laws and DHS privacy policies concerning the operation and maintenance of information systems and programs.
- Recognize and report privacy incidents.
- Assist the Component Privacy Officer/PPOC and the responsible SOC with the development of facts for the Privacy Incident Report.
- Provide advice, expertise, and assistance to the BRT as needed and assist with the investigation and mitigation of a privacy incident.
- Works with employee relations to determine appropriate course of action regarding employee(s) causing privacy incidents.

## DHS Inspector General

- Consult with the DHS Chief Privacy Officer on a case-by-case basis to determine proper incident handling procedures for major privacy incidents.
- Address fraud, abuse, mismanagement, and waste of taxpayer funds invested in Homeland Security, as well as referrals from DHS Chief Privacy Officer on behalf of the BRT.
- Provide advice, expertise, and assistance to the BRT when necessary, and handle privacy incidents in consultation with other members of the team, as requested.
- Provide recommendations to the BRT and Component Head as needed regarding the issuance of notification to third parties.

## United States Computer Emergency Readiness Team (US-CERT)

- Serves as the designated central reporting organization and repository within the Federal Government for federal incident data, communicates and coordinates with the Component Privacy Officer/PPOC to obtain updates regarding the privacy incident, and is responsible for notifying appropriate authorities of the privacy incident, including the Office of Management and Budget (OMB) within one hour of the privacy incident, all in accordance with FISMA.

## Privacy Incident Identification

As soon as a privacy incident is discovered, DHS personnel have an obligation to immediately report the privacy incident to their supervisor, program manager, Component Privacy Officer/PPOC, responsible SOC, or responsible IT Help Desk. If the privacy incident is reported to the program manager, supervisor, or IT Help Desk, the privacy incident must be referred or reported to the Component Privacy Officer/PPOC or responsible SOC in order that the privacy incident will flow through the incident handling process.

Once discovered, DHS personnel should report privacy incidents that are either **suspected and/or confirmed**. A privacy incident involving PII should be viewed as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence when (1) an unauthorized user accesses PII or (2) an authorized user accesses PII for an other than authorized purpose.<sup>13</sup>

In order to encourage effective and efficient responses to privacy incidents, it is imperative not only that the Department train personnel on privacy reporting procedures, but also that it fosters an environment in which individuals feel comfortable reporting a privacy incident. A quick response to

---

13. According to OMB, "common examples of a breach include: a laptop or portable storage device storing PII is lost or stolen; an email containing PII is inadvertently sent to the wrong person; a box of documents with PII is lost or stolen during shipping; an unauthorized third party overhears agency employees discussing PII about an individual seeking employment or federal benefits; a user with authorized access to PII sells it for personal gain or disseminates it to embarrass an individual; an IT system that maintains PII is accessed by a malicious actor; or PII that should not be widely disseminated is posted inadvertently on a public website." OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," p. 9-10.

a newly discovered privacy incident can spare affected individuals adverse consequences as well as save significant time and resources for the Department.

Applicable consequences for failing to comply with safeguarding and reporting requirements can be serious, and may include reprimand, suspension, removal, or other actions in accordance with applicable law and DHS policy. At a minimum, DHS will remove the authority to access information or systems from any individual who demonstrates a disregard or a pattern of not safeguarding PII.

Finally, the DHS Privacy Office, the Component Privacy Officer/PPOC, or the BRT will determine specific details pertaining to an open or closed privacy incident as whether to disclose to any person without an authorized need to know.

### Privacy Incident Reporting: Initial Intake and Opening a Security Event Notification (SEN)

When the privacy incident is identified, the supervisor, program manager, Component Privacy Officer/PPOC, or responsible SOC will need to collect specific information about the nature of the privacy incident to open a suspected or confirmed security event notification (SEN) in the DHS enterprise incident database (ECOP). The SEN, once opened in the ECOP, informs DHS Components about potential malicious activity involving Component Systems.

While not all of the information may be available at the outset, the Component should gather as much information as possible for population of the SEN and update the incident record as facts and information are gathered or revised. This information should include basic facts regarding when the incident occurred and when the incident was discovered, as well as information about the nature of the incident and whether the suspected incident involves PII, including Sensitive PII.

In addition, the Component should also record, in the SEN, any further factual information that will facilitate the handling of the incident as well as actions taken to contain the incident.

### Privacy Incident Reporting

The specific process detailed below is followed during the assessment, analysis, mitigation, and resolution of all privacy incidents, regardless of their designation as major or minor.

Once the determination has been made that a privacy incident is major, there is a shift in the roles and responsibilities *from* the Component Privacy Officer/PPOC *to* the DHS Chief Privacy Officer and the BRT, if convened; otherwise the roles and responsibilities associated with a minor incident remains with the Component Privacy Officer/PPOC and responsible SOC and includes engagement by the DHS Privacy Office, Director of Privacy Incidents as noted in the process flow.

At no time during the process are the DHS Chief Privacy Officer and the Component Privacy Officer/PPOC not engaged in some capacity; rather, it is more a matter of who takes the lead and who takes the supporting role consistent with the designation of the privacy incident as either major or minor.

Once the SEN has been established, the responsible SOC and the Component Privacy Officer/PPOC will then coordinate to gather preliminary information that will become necessary later in the incident handling process. The Component Privacy Officer/PPOC evaluates this information in context and determines whether or not the facts support the conclusion that a privacy incident may have occurred. As part of the initial assessment, the Component Privacy Officer/PPOC will determine whether the incident involves PII, as well as whether the incident involves information from other Components or organizations.

The Component Privacy Officer/PPOC will consult with the Component Chief Security Officer (CSO) when (a) criminal activity is suspected, and (b) the Sensitive PII privacy incident originated or occurred within a classified secured environment (i.e., Closed Storage Processing Area; Open Storage Area; or Sensitive Compartment Information Facility). The Component CSO will determine whether or not to contact law enforcement; confirm the Sensitive PII does not reveal the identity of a confidential human source or a human intelligence source; and avoid potential for a classified spillage.<sup>14</sup>

### Privacy Incident Assessment: PII Determination

The Component Privacy Officer/PPOC will also need to assess the privacy incident to determine whether there are other considerations that require consultation and notice to other Components and DHS stakeholders. To facilitate this assessment, the Component Privacy Officer/PPOC should also consult with the DHS Privacy Office's Director of Privacy Incidents.

The Component Privacy Officer/PPOC will need to determine whether Sensitive PII was involved. In addition to Sensitive PII, the Component Privacy Officer/PPOC should consult the Component program manager and SOC to determine if certain financial and/or certain health information was involved, if the incident was caused by a contractor, if the incident involved information from multiple components, or if criminal activity is suspected.

Incident assessment factors include:

#### i) Sensitive PII<sup>15</sup>

The Component Privacy Officer/PPOC should determine whether the incident involves Sensitive PII. Sensitive PII is personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

Sensitive PII requires stricter handling guidelines because of the increased risk to an individual if the data is compromised. Some categories of PII are sensitive as stand-alone data elements, including a Social Security number (SSN) or driver's license or state identification number. Other data elements such as citizenship or immigration status, medical information, ethnic, religious, sexual orientation, or lifestyle information, in conjunction with the identity of

---

14. DHS Instruction 121-01-011, "The Department of Homeland Security Administrative Security Program", Chapter 2.E.3(c) and (d).

15. See DHS Privacy Policy Directive 140-10, "Handbook for Safeguarding Sensitive Personally Identifiable Information."

an individual (directly or indirectly inferred), are also Sensitive PII.

In many instances, the Component Privacy Officer/PPOC must use a best judgment standard in assessing the sensitivity of PII in its context. For example, an office contact list contains PII (e.g., name, phone number). In this context, the information probably would not be considered sensitive. However, the same information in a roster of law enforcement personnel probably would be considered sensitive information. In assessing the levels of risk and harm, consider the data element(s) in light of their context and the broad range of potential harms flowing from their disclosure to unauthorized individuals.

#### ii) Contractor Obligations

The PIHG applies to all DHS personnel, including contractors. Contractors are obligated to comply with all DHS privacy policies and procedures. For the purposes of privacy incident handling, contractor responsibilities are nearly identical to those of a DHS employee. Contractors should report incidents to departmental program supervisors or managers, Component Privacy Officers/PPOCs, or responsible SOC. However, contractors must also report any privacy incident to their official Contracting Officer's Representative (COR). Moreover, the Component Privacy Officer/PPOC and SOCs must continue to consult and work through the COR regarding any matters regarding the contractor.

At this stage, the COR and the Component Privacy Officer/PPOC should review the contract for inclusion of the contractor's breach notification or incident response responsibilities. These responsibilities are described in the Homeland Security Acquisition Regulations.<sup>16</sup>

#### iii) Financial Information

The Component Privacy Officer/PPOC should also determine, to the extent possible and at the earliest stage of the privacy incident, whether the privacy incident involves government-issued credit cards or individuals' financial information, such as bank account numbers used for direct deposit of credit card reimbursements, or any benefit information. If so, the Component Privacy Officer/PPOC should immediately notify the Component or DHS Office of the Chief Financial Officer (CFO). The Component or DHS CFO will notify the affected bank(s), the Office of the Chief Human Capital Officer (CHCO), and the Component CHCO. The Component Privacy Officer/PPOC will update the Privacy Incident Report to reflect the CFO's notification of the affected bank(s).

Escalation to the CFO is warranted when the privacy incident involves CFO Designated Financial Systems. DHS CFO Designated Financial Systems are systems that require additional management accountability and effective internal control over financial reporting.

---

16. The [Homeland Security Acquisition Regulation](#) requires clauses be included in DHS solicitations and contracts to address contractor responsibilities for reporting and responding to breaches. These HSAR clauses include 3052.204-70, Security Requirements for Unclassified Information Technology Resources (June 2006); 3052.204-71, Contractor Employee Access (Sept. 2012); and special clauses Safeguarding of Sensitive Information (Mar. 2015) and Information Technology Security and Privacy Training (Mar. 2015) from HSAR Class Deviation 15-01, Safeguarding of Sensitive Information.

The DHS Chief Privacy Officer may also request the Component or DHS CFO and CHCO to be included as representatives to the Breach Response Team (BRT) as necessary.

#### iv) Health Information

The Component Privacy Officer/PPOC should also determine, to the extent possible and at the earliest stage of the privacy incident, whether the privacy incident involves individually identifiable health information, such as demographic data, that relates to:<sup>17</sup>

- the individual's past, present, or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.
- individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security number).

Incidents involving HIPAA are to be reported to the U.S. Department of Health and Human Services Office for Civil Rights as necessary.

#### v) Multiple Components

The Component Privacy Officer/PPOC should also determine whether the privacy incident involves PII from multiple Components. The Privacy Incident Report should accurately reflect the information and Components affected as well as being designated in the ECOP as a multiple component privacy incident. The Component Privacy Officer/PPOC may also work through the DHS Chief Privacy Officer and DHS Privacy Office to communicate with the other Component Privacy Officers/PPOCs about the privacy incident to ensure they are aware of the incident and the mitigation and remediation in the Components is consistent.

### Privacy Incident Assessment: US-CERT - DHS SOC and Official Notice to DHS Officials

When the results of the Incident Assessment confirm a privacy incident, escalation is recommended, and the status should change in the ECOP from a SEN to an Incident. Further, the DHS SOC must transmit the Incident Report to the United States Computer Emergency Readiness Team (US-CERT), which serves as the designated central reporting organization and repository within the Federal Government for federal incident data and automatically forwards notification to OMB as well as appropriate authorities.

---

17. Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). See 45 CFR Part 160 and 164, Subparts A and E (HIPAA Privacy Rule). More information can be found here: <https://www.hhs.gov/hipaa/index.html>.

## Privacy Incident Reporting: Distinguishing between Minor and Major Incidents

Once the privacy incident is reported to US-CERT, the Component Privacy Officer/PPOC determines whether the privacy incident is a major incident,<sup>18</sup> which requires congressional notification,<sup>19</sup> or a minor incident.

A minor incident is defined as “an incident that due to proper functioning of a security control is not likely to impact the DHS mission or a critical DHS asset. Minor incidents do not require immediate leadership notification. Further, a minor incident meets one or more of the following criteria:

- The incident impacts the confidentiality, integrity, or availability of a non-critical system or non-sensitive data.
- The incident relates to a minor policy violation.”<sup>20</sup>

A privacy incident constitutes a major privacy 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 privacy incident.<sup>21</sup>

OMB M-18-02 defines a breach that constitutes a major incident as follows:

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.”

Subsequent OMB Guidance may change or alter this definition.

---

18. 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.

19. See 44 U.S.C. § 3554(b)(7). A Department official, (i.e., DHS Chief Privacy Officer reports breaches, and the DHS Chief Information Officer reports non-breaches), 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. In addition, the Department supplements its 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. Further, if the Department determines a “major incident” has occurred, US-CERT is required to notify OMB within one hour of US-CERT being so alerted.

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

21. Pursuant to OMB M-18-02, FISMA Guidance, section II. This definition may change since OMB issues new FISMA guidance each year.

The DHS Chief Privacy Officer, in coordination with the CIO and CISO, will first determine whether the privacy incident is considered a “major incident” that involves PII.

There are several criteria to evaluate in this definition and there may be instances in which a privacy incident may meet the criteria above but not affect 100,000 or more individuals' PII. Those instances are no less significant any may indeed warrant the convening of the BRT by the DHS Chief Privacy Officer.

It is for this reason that during the incident assessment phase, the Component Privacy Officer/PPOC be cognizant of whether the incident meets the definition of a major privacy incident and not look at applying the classification of the privacy incident **only** because the 100,000 affected individuals' PII threshold is met.

To facilitate this determination, the Component Privacy Officer/PPOC will identify the system of records notice (SORN), privacy impact assessment (PIA), and/or other existing compliance documents that may apply to the compromised PII or SPII. The Component Privacy Officer/PPOC will provide this information to the DHS Chief Privacy Officer and the Director of Privacy Incidents at the Privacy Office.

Once the determination has been received, the DHS Chief Privacy Officer, in coordination with the CIO and CISO, will validate whether the privacy incident is a major incident that involves PII.

## Congressional Notification

If the privacy incident is validated as a major incident that involves PII, the DHS Chief Privacy Officer must notify appropriate congressional committees no later than seven days after the date on which DHS has reasonably concluded that a major privacy incident occurred. The DHS Chief Privacy Officer must supplement that seven day notification to Congress with updates within a reasonable period of time. In addition, DHS Chief Privacy Officer must also supplement the seven day notification with a report no later than 30 days after a major privacy incident is discovered. The DHS Chief Privacy Officer will coordinate with OLA, as a member of the Breach Response Team, as described below, for such notification to these committees.<sup>22</sup>

## Convening the Breach Response Team (BRT)

Once the DHS Chief Privacy Officer validates, after consultation with the CIO and CISO, a major privacy incident has occurred, the DHS Chief Privacy Officer may convene the DHS BRT.<sup>23</sup> If activated, the BRT is convened within 72 hours.

The BRT will conduct the investigation of the major incident and the subsequent actions, or direct the DHS Privacy Office or the Component Privacy Officer/PPOC to coordinate the investigation within

---

22. See DHS Instruction 047-01-006 Privacy Incident Responsibilities and Breach Response Team.

23. As defined in OMB M-17-12, a “breach response team is the group of agency officials designated by the head of the agency that may be convened in response to a breach.” For instruction and guidance concerning the DHS Breach Response Team, see *DHS Instruction 047-01-006, Privacy Incident Responsibilities and Breach Response Team*

the Component, depending on the nature of the privacy incident. If the DHS Chief Privacy Officer decides to convene the BRT, then the DHS Privacy Office will coordinate the activities associated with the technical investigation. Please note that in the event of a minor privacy incident, the Component Privacy Officer/PPOC will conduct investigative activities regarding the incident at the Component level.

The BRT is responsible for advising the DHS Chief Privacy Officer and Department leadership on effectively and efficiently responding to the privacy incident, including assessing the risk of harm to individuals, considering potential mitigations, implementing notification to affected individuals, and discussing lessons learned. The BRT is composed of senior Department and Component officials, or their representatives, who may be convened to respond to the privacy incident.

The BRT includes, at a minimum, the following officials or their representatives:

- DHS Under Secretary for Management
- DHS CIO
- DHS CISO
- DHS General Counsel
- Assistant Secretary for Public Affairs
- Assistant Secretary for Legislative Affairs
- Affected Component Personnel:
  - Component IT Security Entity (e.g., Component Information Systems Security Manager (ISSM), Computer Security Incident Response Center (CSIRC), SOC for the Component);
  - Component Privacy Officer or Privacy Point of Contact (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; and
  - Component CFO;

As necessary, depending on the type of incident, the DHS Chief Privacy Officer may request additional subject matter experts to join and assist the BRT. For example, if the privacy incident involves financial information, the DHS Chief Privacy Officer may request the DHS Chief Financial Officer to join the BRT.

## Assessing the Risk of Harm to Individuals Impacted by a Privacy Incident (Risk

---

24. The DHS PIHG utilizes the "Factors for Assessing the Risk of Harm to Potentially Affected Individuals," from OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information." (Jan. 3, 2017). Minor modifications were made to this assessment framework to reflect specific DHS roles and responsibilities, as well as other considerations. OMB M-17-12 provides a "Model Breach Reporting Template" that includes many elements that can assist in the risk assessment, p. 38-41.

## Assessment)<sup>24</sup>

All privacy incidents require a technical investigation, in addition to the facts gathered at the initial incident intake, in order to collect the information required to conduct a risk assessment and propose appropriate mitigations.

In any privacy incident involving PII, DHS must assess the risk of harm to individuals impacted by a privacy incident. This assessment is based on three factors:

- Nature and sensitivity of the PII
- Likelihood of access and use of PII
- Type of Privacy Incident

While the DHS Chief Privacy Officer is ultimately accountable for ensuring the assessment of the risk of harm to individuals, the following considerations and evaluations will be carried out for major or minor privacy incidents either by the BRT (overseen by the DHS Privacy Office, Director of Privacy Incidents), or the Component Privacy Officer/PPOC. A thorough risk assessment will help identify appropriate mitigation measures. The assessment also helps support the production of materials that may be needed to facilitate notification. It is important to remember, however, that the results of the assessment and any recommendations must be provided to the DHS Chief Privacy Officer, who provides recommendations to the Secretary regarding the issuance of notification to affected individuals, including the timeliness, contents, means, sources, and general appropriateness of the notification.

The range of potential harms associated with the loss or compromise of PII is broad. A number of possible harms associated with the loss or compromise of PII must be considered. Such harms may include:

- The effect of a breach of confidentiality or fiduciary responsibility
- The potential for blackmail
- The disclosure of private facts, mental anguish, and emotional distress
- The disclosure of address information for victims of abuse
- The potential for secondary uses of the information that could result in fear or uncertainty
- The unwarranted exposure leading to humiliation or loss of self-esteem

Finally, as with other tasks, it is also important for the Component Privacy Officer/PPOC to update the enterprise incident database as to the risk assessment findings.

### *Assessing the Risk of Harm*

#### i) Nature and Sensitivity of PII

When assessing the nature and sensitivity of compromised PII with a privacy incident, the BRT or the Component Privacy Officer/PPOC should consult the relevant DHS and Component stakeholders to consider the following:

#### a) Data Elements

Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual (e.g., SSN, passport number, driver's license number, bank account numbers, biometric identifiers). The BRT or the Component Privacy Officer/PPOC should consider the sensitivity of all of the data elements, taken

together. While none of the information may be sensitive in isolation, it can pose a great risk of harm to individuals after being combined together. For example, date of birth, place of birth, address, and gender may not be particularly sensitive alone, but when combined would pose a greater risk of harm to the individual.

Finally, the BRT or Component Privacy Officer/PPOC should consider how many records are involved and whether individuals could be identified by the information involved. Privacy incidents of 25 records and 25 million records may have different impacts, not only in terms of the collective harm to individuals, but also in terms of harm to the Component's reputation.

#### b) Context

The BRT or Component Privacy Officer/PPOC must also consider the purpose for which the PII was collected, maintained, and used. The same information in different contexts can reveal additional compromising information about impacted individuals. For instance, a list of personnel and their associated office phone numbers may not be particularly sensitive. However, the same list of personnel and their associated office phone numbers on a list of personnel who hold sensitive positions within a law enforcement agency is sensitive information. A similar list of names and phone numbers along with information about a medical condition is also sensitive.

#### c) Private Information

The BRT or Component Privacy Officer/PPOC must evaluate the extent to which the PII constitutes information that an individual would generally keep private or chooses to keep private. Such "private information" may not present a risk of identity theft or other criminal conduct, but may pose a risk of harm such as embarrassment, blackmail, or emotional distress. Examples include information that a person may choose not to share with others, yet the Department has collected such as: derogatory personal or criminal information, personal debt, medical conditions, treatment for mental health, pregnancy-related information, sexual history or sexual orientation, adoption or surrogacy information, and immigration status. Passwords are another example of private information that if involved in a privacy incident may present a risk of harm.

#### d) Vulnerable Populations

The BRT or Component Privacy Officer/PPOC must consider whether the affected individuals are from a particularly vulnerable population that may be at greater risk of harm than the general population and if the information involved somehow increases the risk of harm to that population. In fact, part of the vulnerability may simply be having any information about the persona known. Vulnerable populations include: children; active duty military; government officials in sensitive positions; senior citizens; individuals with disabilities; confidential informants; witnesses; certain populations of immigrants; non-English speakers; and victims of certain crimes such as identity theft, child abuse, trafficking, domestic violence, or stalking. This is not a comprehensive list and other populations may also be considered vulnerable.

#### e) Permanence

Finally, the BRT or Component Privacy Officer/PPOC shall consider the permanence of the PII. This includes an assessment of the relevancy and utility of the information over time and whether the information will permanently identify an individual. Some information loses its relevancy or utility as it ages, while other information is likely to apply to an individual throughout his or her life. For example, an individual's health insurance ID number can be replaced. However, information about an individual's health, such as family health history or chronic illness, remains relevant for an individual's entire life, as well as the lives of his or her family members.

Special consideration is warranted when a privacy incident involves biometric information including fingerprints, facial images, hand geometry, retina or iris scans, and DNA or other genetic information. When considering the nature and sensitivity of biometric information, a Component should factor in the known current uses of the information and consider that, with future advancements in science and technology, biometric information could have many additional and sensitive uses not yet contemplated.

#### ii) Likelihood that PII is Accessible and Usable

When assessing the likelihood of access and use of PII compromised by a privacy incident, the BRT or Component Privacy Officer/PPOC should consider the following:

##### a) Security Safeguards

The fact that the information has been lost or stolen does not necessarily mean it has been or can be accessed depending on the physical, technological, and procedural safeguards employed by the Component. If the information is properly protected by a NIST-compliant encryption method, the actual risk of compromise is low to non-existent.

The BRT or Component Privacy Officer/PPOC should consult the DHS or Component CISO to evaluate the implementation and effectiveness of implemented security safeguards, such as password protection or encryption, protecting the information. Security safeguards may significantly reduce the risk of harm to affected individuals, even when the PII is particularly sensitive. The CISO shall consider each of the employed security safeguards on a case-by-case basis and takes into account whether the type, value, or sensitivity of the information might motivate a malicious actor to put time and resources towards overcoming those safeguards.

Encryption can be an effective safeguard, and can be applied at the device-level, file-level, or to information that is at rest or in transmission. Encryption protections may be undermined if keys, credentials, or authenticators used to access encrypted information are compromised. When evaluating the likelihood of access and use of encrypted PII, the BRT or Component Privacy Officer/PPOC should consult with the CISO and other technical experts to ascertain whether information was properly

encrypted, including:

- Whether encryption was in effect
- The degree of encryption
- At which level the encryption was applied
- Whether decryption keys were controlled, managed, and used.<sup>25</sup>

There are other effective security safeguards, apart from encryption. Redaction, data-masking, and remote wiping of a connected device can partially or completely block access to PII. A review of security logs can help to confirm whether there was access to data, and in some cases, which Internet Protocol (IP) addresses were associated with that access. Physical security safeguards such as a locked case may also reduce the likelihood of access and use of PII.

#### b) Format and Media

The BRT or Component Privacy Officer/PPOC, in coordination with the DHS or Component CIO/Component SOC representatives, shall evaluate whether the format or media of the PII may make its use difficult and resource-intensive. The format of the PII or the media on which it is maintained may make the PII more susceptible to a crime of opportunity. For example, a spreadsheet on a portable USB flash drive does not require any special skill or knowledge to access and an unauthorized user could quickly search for specific data fields such as a nine-digit SSN. Conversely, a magnetic tape cartridge used for backing up servers that is one of a set of 30 and contains a large volume of unstructured PII would require special expertise or equipment to access and use the information.

As part of this assessment, the BRT or Component Privacy Officer/PPOC will also need to consider the type, value, and sensitivity of the PII. If the PII is particularly valuable, it may increase the likelihood of access and use regardless of its format or media. This is because the value of the information may outweigh the difficulty and resources needed to access the information.

#### c) Duration of Exposure

The BRT or Component Privacy Officer/PPOC must determine the amount of time that the PII was exposed or make a reasonable estimate of this time. PII that was exposed for an extended period of time is more likely to have been accessed or used by unauthorized users. For example, a briefcase containing PII left in a hotel lobby or a car for an hour before being recovered is less likely to have been accessed by an unauthorized user than if it had been left for three days prior to being recovered. Similarly, PII inadvertently published to a public Internet page for an hour before being removed is less likely to have been accessed by an unauthorized user than if it

---

25. OMB M-17-12 notes that “[f]ederal agencies are required to use a NIST-validated encryption method.” OMB Circular A-130, Appendix I-13, requires agencies to “[e]ncrypt all FIPS 199 moderate-impact and high-impact information at rest and in transit, unless encrypting such information is technically infeasible or would demonstrably affect the ability of agencies to carry out their respective missions, functions, or operations; and the risk of not encrypting is accepted by the authorizing officials and approved by the agency CIO, in consultation with the Senior Agency Official for Privacy (SAOP) (as appropriate).

had been available on the public Internet page for a week.

#### d) Evidence of Misuse

The BRT or Component Privacy Officer/PPOC must determine whether there is evidence of misuse. In some situations, the Component may be able to determine with a high degree of certainty that PII has been or is being misused. Evidence may indicate that identity theft has already occurred as a result of a specific or that the PII is appearing in unauthorized external contexts. For example, law enforcement may confirm that PII is appearing on a website dedicated to the sale of stolen PII and may determine that there is strong evidence of misuse. Conversely, agencies may determine with reasonable certainty that the PII will not be misused. For example, a forensic analysis of a recovered device may reveal that the PII was not accessed. Or, PII compromised by a privacy incident may also be rendered partially or completely inaccessible by security safeguards other than encryption through redaction or remote wiping of a connected device.<sup>26</sup> Physical security safeguards, such as a locked cabinet or locked briefcase, will also be considered.

### iii) Type of Privacy Incident

The BRT or Component Privacy Officer/PPOC will consider the whether the major or minor privacy incident was intentional, who received the information, and whether the intent is unknown.

#### a) Intent

If a privacy incident was intentional, it is important to determine whether the information was the target, or whether the target was the device itself, like a mobile phone or laptop, and whether the compromise of the information was incidental. Examples of an intentional privacy incident include the theft of a device storing PII from a car or office, the unauthorized intrusion into a Government network that maintains PII, or an employee looking up a celebrity's file in a Component database out of curiosity. While the risk of harm to individuals may often be lower when the information was not the target, the potential for a significant risk of harm to individuals may still exist.

The risk of harm to individuals may be lower when a privacy incident is unintentional, either by user error or by failure to comply with DHS policy. However, that is not always the case, and privacy incident response officials must conduct a case-by-case assessment to determine the risk of harm. Examples of an unintentional privacy incident include an employee accidentally emailing another individual's PII to the wrong email address or a contractor storing personnel files in a shared folder that the contractor thought was access-controlled but was not.

It may be impossible or impractical to determine whether a privacy incident was intentional or unintentional. In these instances, the BRT or Component Privacy Officer/

---

26. See DHS 4300A Sensitive Systems Handbook, Attachment F to Handbook Version 11.0, Incident Response, Ver. 11.0, April 24, 2015

PPOC should operate on the assumption that the privacy incident was intentional. For example, if an employee realizes her mobile device is missing, it may be that it was stolen intentionally or that she dropped it accidentally. Similarly, a shipment containing A-Files that never arrives at its destination may have been unintentionally lost or may have been targeted by a malicious actor and intercepted.

#### b) Criminal Activity

If the initial fact gathering suggests potential criminal activity, the Component Privacy Officer/PPOC should immediately notify and coordinate with the responsible SOC or the DHS SOC Government Watch Officer. External notification to law enforcement when criminal activity is suspected or confirmed should be handled by the Component CSO and/or DHS CSO depending on the level and severity of criminal activity.

Notification and involvement of external law enforcement must be documented in the Privacy Incident Report. The Chief Privacy Officer may also report suspected fraud to the DHS Inspector General.

Furthermore, in circumstances when law enforcement has been notified of a privacy incident, the BRT or Component Privacy Officer/PPOC shall consider any relevant information provided by law enforcement that may help inform whether the privacy incident was intentional or unintentional.

#### c) Recipient

In some cases, the Component may know who received the compromised PII. This information, when available, may help the BRT or Component Privacy Officer/PPOC assess the likely risk of harm to individuals. For example, a privacy incident is often reported by a recipient who receives information he or she should not have received. This may be an indication of a low risk of harm to individuals, particularly when the recipient is another employee within the Component's IT network. One common type of low-risk privacy incident is when an employee sends an individual's PII via email to another employee at the same Component who does not need to know that PII in order to perform his or her duties. In many such cases it may be reasonable to conclude that there is a negligible risk of harm. Even when PII is inadvertently sent to an individual outside DHS, the risk of harm may be minimal if it is confirmed that, for example, the individual is known to the Component, acknowledged receipt of the PII, did not forward or otherwise use the PII and the PII was properly, completely, and permanently deleted by the recipient. This is a type of privacy incident that must be reported by the Component and must appropriately respond, but the risk of harm is low enough that the response often may not necessitate that the Component notify or provide services to the affected individual whose PII was compromised.

Conversely, if analysis reveals that the PII is under the control of a group or person who is either untrustworthy or known to exploit compromised information, the risk of harm to the individual is considerably higher. In many cases the Component will not have any information indicating that compromised or lost PII was ever received or acquired by anyone. In such circumstances, the BRT or Component Privacy Officer/

PPOC shall rely upon the other factors considered.

### Assessing Priority

Once the Component Privacy Officer/PPOC and/or the responsible SOC opens the SEN, the responsible SOC will then assign a priority to the incident in accordance with *DHS Sensitive Systems Policy Handbook, 4300A (Attachment F, "Incident Response")* and the Component Privacy Officer/PPOC will consider the Standards for Categorization of Privacy Incidents detailed below is assigning a risk of harm to the incident.

#### The likely risk of harm is LOW if the Privacy Incident:

- Could result in limited or no harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained; or
- Could have a limited or no adverse effect on organizational operations or organizational assets.

#### The likely risk of harm is MODERATE if the Privacy Incident:

- Could result in significant harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained; or
- Could have a serious adverse effect on organizational operations or organizational assets.
- Sensitive PII is always designated as moderate or high impact.

#### The likely risk of harm is HIGH if the Privacy Incident:

- Could result in severe or catastrophic harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained;
- Could have a severe or catastrophic adverse effect on organizational operations or organizational assets; or,
- Sensitive PII is always designated as moderate or high impact.

### Mitigation

Mitigation is an essential aspect of DHS's effort to contain the cause of the major or minor privacy incident, and identify and lessen the potential harm that the loss, compromise, or misuse of the PII may have on affected individuals.

Once the risk of harm has been thoroughly assessed, the BRT or Component Privacy Officer/PPOC should identify and recommend appropriate mitigations to the DHS Chief Privacy Officer, in the case of a major privacy incident, or to his/her Component in the case of a minor privacy incident. Mitigations may range from technical countermeasures, which must be coordinated through the DHS SOC or responsible SOC, to non-technical activities, such as notification and/or credit monitoring to the affected individuals and employee counseling, as well as to engagement with the DHS Office of Inspector General and other law enforcement entities.

The DHS SOC or responsible SOC will conduct technical countermeasures to address IT security issues relevant to the privacy incident, if appropriate.<sup>27</sup>

The BRT or Component Privacy Officer/PPOC should also address the privacy ramifications of a privacy incident, focusing on preventing or minimizing any subsequent harm to affected individuals. As such, non-technical privacy mitigations will involve activity beyond the securing of the system (electronic or paper) and isolating the vulnerability.

The BRT or Component Privacy Officer/PPOC should include a broad range of mitigation strategies based on the nature and sensitivity of the PII involved. An effective response may call for disclosure of information regarding a privacy incident to those individuals affected by it, as well as to persons and entities in a position to cooperate, either by assisting in notification to affected individuals or playing a role in preventing or minimizing harms from the privacy incident. Mitigations may include:

- Notification to affected individuals, the public, media, and other Government entities (e.g., Congress).
- Removing information from an Internet or Intranet page.
- Offering credit or identity monitoring services or providing information on such services to mitigate the misuse of the PII and identify patterns of suspicious behavior.
- Training and awareness for staff on best practices to safeguard Sensitive PII.
- Disciplinary or corrective action, including counseling for DHS employees. *NOTE:* any DHS personnel subject to corrective or disciplinary action arising out of a privacy incident must not be identified or identifiable in the Privacy Incident Report. The privacy incident report should simply contain a statement that corrective or disciplinary action was taken without providing identifiable information about the employee(s) involved and without providing any specifics. The respective Component Human Capital Office must maintain a record of all disciplinary or corrective actions taken against DHS personnel that arise out of a privacy incident.
- Revisions to policies and procedures to minimize or eliminate the use of PII when possible.
- Contractors must comply with Department policies and follow all aspects of the HSAR clauses, FAR clauses, and/or privacy provisions that are included in the contract, such as allowing Department inspection provisions and post-incident activities.

## Notification for a Privacy Incident

---

27. For more information about potential mitigations, consult DHS 4300A Sensitive Systems Handbook, Attachment F to Handbook Version 11.0, Incident Response, Ver. 11.0, April 24, 2015

In the case of a major privacy incident, once the BRT or the Component Privacy Officer/PPOC has conducted the risk assessment and has identified potential mitigations, recommendations should be provided to the DHS Chief Privacy Officer in the case of a major privacy incident and the privacy incident report should be updated.

In the context of a major privacy incident, and as part of the effort to ensure substantive and effective notification, the DHS Chief Privacy Officer will solicit input from the BRT, including the DHS Office of the General Counsel (OGC), Office of Public Affairs (OPA), and Office of Legislative Affairs (OLA), as well as the Component Privacy Officer/PPOC in assessing the following issues:

- Timeliness of the Notification
- Source of the Notification
- Contents of the Notification
- Means of Providing the Notification
- Who Receives Notification: Public Outreach in Response to a Privacy Incident

After receiving input from the BRT or the Component Privacy Officer/PPOC, the DHS Chief Privacy Officer provides recommendations to the Secretary regarding the issuance of notification to affected individuals, including 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.

Further, the DHS Chief Privacy Officer or DHS Privacy Office, Director of Privacy Incidents, may need to coordinate with DHS OPA to provide *reasonable advance internal notice* to DHS senior officials by email or voicemail of a notification decision before external notification.

In the case of a minor privacy incident, once the Component Privacy Officer/PPOC has conducted the risk assessment and identified potential mitigations, the Privacy Incident Report should be updated. The assessment regarding notification to the affected individual(s) will take into account many, if not all, of the same issues considered in notification for major privacy incidents. The Privacy Incident Report should also detail a recommendation regarding notification to affected individuals.

#### i) [Timeliness of Notification for a Privacy Incident](#)

Before notification may be issued, DHS must first determine the scope of the privacy incident, and if applicable, restore the reasonable integrity of the system or information compromised. Affected individuals shall be notified without unreasonable delay following the discovery of a major privacy incident, consistent with the needs of law enforcement and national security, and any measures necessary for DHS to assess the scope of the privacy incident and implement containment measures.

In some circumstances, law enforcement or national security considerations may require a delay in notification if it impedes the investigation of the privacy incident, as permitted by OMB Memorandum M-17-12.<sup>28</sup> Decisions to delay notification should be made by the DHS Secretary or a senior-level official designated by the Secretary *in writing* (emphasis added).

---

28. OMB M-17-12, p. 31.

## ii) Source of Notification for a Major Privacy Incident

As a general rule, notification to affected individuals for all minor privacy incidents will be issued by the Component Head or the Component Privacy Officer/PPOC, if appropriate; or if warranted by the circumstances, the DHS Privacy Office, Director of Privacy Incidents, may issue the notice to individuals affected by the privacy incident.

In the case of a major privacy incident, the DHS Chief Privacy Officer provides recommendations to the Secretary regarding the issuance of notice, including timeliness, content, means, sources and general appropriateness, as described above.

When the privacy incident involves a federal contractor or a public-private partnership maintaining PII on behalf of the Component, DHS is ultimately responsible for ensuring that any notification and corrective action is taken by the contractor. The roles, responsibilities, and relationships with contractors or partners should be reflected in the system certification and accreditation (C&A) documentation, as well as contracts and other documents (e.g., HSAR Clauses). The DHS Chief Privacy Officer and DHS Privacy Office should be engaged in all contractor-related notification and corrective action.

## iii) Contents of the Notification for a Privacy Incident

With a minor privacy incident, the Component Privacy Officer/PPOC will leverage existing notification templates and address the following factors, if appropriate. In the case of a major privacy incident, the following elements, amended for the circumstances, should be included:

- Brief description of what happened, including the date(s) of the privacy incident and of discovery.
- To the extent possible, a description of the types of personal information involved in the privacy incident (e.g., full name, SSN, date of birth, home address, account number, Alien Registration Number/file).
- Statement whether the information was encrypted or protected by other means, when determined that such information would be beneficial, and would not compromise the security of the system.
- Steps/Guidance individuals can take to protect themselves from potential harm.
- What the Component or DHS is doing to investigate the privacy incident, mitigate losses, and protect against a likely recurrence.
- Who affected individuals should contact at the Component or DHS for more information, including a telephone number, email address, or postal address.

In addition to the specifics of the notification, it is also important to consider supplemental materials that may facilitate substantive and effective notice.

In the event of a major privacy incident, the following factors may also need to be considered:

a) **Translation of Notice into Other Languages or Formats**

Effective privacy incident handling necessitates that individuals affected by the privacy incident understand the importance of the notification. Therefore, if the Component's records show that the affected individuals are not English speaking, notice should also be provided in the appropriate language(s). If agencies have knowledge that the affected individuals are not English speaking, or require translation services, the Component should also provide notification in the appropriate languages to the extent feasible.

Special consideration should be given to provide notification to individuals who are visually or hearing impaired consistent with Section 508 of the Rehabilitation Act of 1973. Accommodations may include establishing a telecommunications device for the deaf (TDD) or posting a large type notice on the DHS or affected Component's Internet or Intranet website.

b) **Frequently Asked Questions**

A Frequently Asked Questions (FAQ) format on the DHS or Component Internet or Intranet webpage may be beneficial because this information can be easily updated, contain links to more information, provide more tailored information than the formal notification, and can be easily translated into multiple languages. The Internet webpage also helps support requirements to provide information to visually impaired individuals as required by Section 508 of the Rehabilitation Act.<sup>29</sup>

c) **Call Center**

For a privacy incident that affects a large number of individuals, or as otherwise appropriate, agencies should establish toll-free call centers staffed by trained personnel to handle inquiries from the affected individuals.

iv. **Methods/Mean of Providing the Notification**

An important aspect of substantive and effective notification for a privacy incident is the selection of the method for providing notification. The best method for providing notification will depend on the number of individuals affected, the available contact information for the affected individuals, and the urgency with which the individuals need to receive the notification. The following examples are types of notices that may be considered:

a) **First-Class Mail**

First-class mail notification to the last known mailing address of the individual in DHS records should be the primary means to provide notice. When the Component has reason to believe the address is no longer current, it should take reasonable steps to update the address by consulting with other agencies such as the U.S. Postal Service. The notification should be sent separately from any other mailing so that it is

---

29. See 30 U.S.C. § 794 (d).

conspicuous to the recipient. If the Component that experienced the privacy incident uses another Component to facilitate mailing, it should take care to ensure that the Component that suffered the loss is identified as the sender. The front of the envelope should be labeled to alert the recipient to the importance of its contents and should be marked with the name of either DHS or the Component as the sender to reduce the likelihood the recipient thinks it is advertising mail. Components should anticipate that some mail will be returned as undeliverable and should have procedures in place for how to provide a secondary notification.

#### b) Telephone

Telephone notification may be appropriate in those cases when urgency may dictate immediate and personal notification, and/or when a limited number of individuals are affected. Telephone notification, however, should be followed by written notification by first-class mail.

#### c) Email

While the DHS Chief Privacy Officer does not recommend email as the primary form of notification, in limited circumstances it may be appropriate. Email notification, especially to or from a non-Government email address, is not recommended due to the high risk of malicious email attacks that are often launched when attackers hear about a privacy incident (e.g., phishing). Emails often do not reach individuals because they are automatically routed to spam or junk mail folders. Individuals who receive notifications via email are often uncertain of the legitimacy of the email and will not open the notification.

If the individuals affected by a privacy incident are internal to the Department, it may be appropriate for DHS to use an official email address to notify a small number of employees, contractors, detailees, or interns via their official email addresses.

#### d) Substitute Notice

In the event there is not sufficient contact information to provide notification, or in the case of supplemental notification for a privacy incident to keep affected individuals informed as to new facts, the DHS Chief Privacy Officer may choose substitute notice.

This type of notice may also be beneficial when DHS or the Component needs to provide an immediate or preliminary notification in the wake of a high-profile privacy incident when notification is particularly time-sensitive. A substitute notification should consist of a conspicuous posting of the notification on the home page of DHS's or the Component's Internet or Intranet website and/or notification to major print and broadcast media, including major media in areas where the affected individuals reside. Notification to media should include a toll-free phone number and/or an email address that an individual can use to learn whether or not his or her personal information is affected by the privacy incident.

In instances when there is an ongoing investigation and the facts and circumstances of a privacy incident are evolving, Components should consider whether it is appropriate to establish an ongoing communication method for interested

individuals to automatically receive updates. Depending on the individuals affected and the specific circumstances of a privacy incident, it may be necessary for Components to provide notifications in more than one language.

#### e) Accommodations/Special Considerations

When a privacy incident affects a vulnerable population, DHS or the Component may need to provide a different type of notification to that population, or provide a notification when it would not otherwise be necessary.

There may be instances when a Component provides notification to individuals other than those whose PII was compromised. For example, when the individual whose information was compromised is a child, the Component may provide notification to the child's legal guardian(s). Special care may be required to determine the appropriate recipient in these cases.

#### f) Webpage

The webpage posting should provide:

- Summary of incident with a clear introduction (who, what, when, why, where, how) that articulates what has happened and what DHS is asking of the public (or DHS employees);
- A background section with more detailed info;
- A resources section with tools and helpful information resources for people to reference;
- FAQs; and
- Call center number, if applicable

Component Privacy Officers/PPOCs may want to also consider developing and publishing a page on DHS Connect and your Component's Intranet page with the same information.

#### v) Who Receives Notification

The final consideration in the notification process for a major or minor privacy incident is to whom DHS and its Components should provide notification beyond the affected individuals, such as the media, and/or other third parties affected by the privacy incident or the notification. Unless notification to individuals is delayed or barred due to law enforcement or national security reasons, all affected individuals should receive prompt notification.

DHS and its Components should consider the following guidelines when communicating with third parties regarding a privacy incident:

##### a) Media

The decision to notify the media regarding a privacy incident requires careful planning and execution so as not to unnecessarily alarm the public. When appropriate, the media should be notified as soon as practicable after the discovery of an incident and informed that a handling plan, including the notification, has been developed. Notification should focus on providing information, including links to

resources, to aid the public in its response to the privacy incident. In addition, the FTC should be offered as a resource for affected individuals to confirm the legitimacy of the notification. Law enforcement or national security agencies may request that DHS or its Component(s) delay notification as described above. To the extent possible, prompt public media disclosure is generally preferable because delayed notification may erode public trust. Contact with the media should be coordinated through DHS Office of Public Affairs or the Component's Office of Public Affairs.

DHS can post information about the privacy incident and notification in a prominent location on the DHS homepage or the Component's Internet or Intranet website as soon as possible after the discovery of a privacy incident, and the decision to provide notification to the affected individuals. The posting should include a link to FAQs and other relevant materials regarding the incident.

#### b) Third Parties Affected by the Privacy Incident

The Component Head and Component Privacy Officer/PPOC for the affected Component must work in consultation with the DHS Chief Privacy Officer to determine whether other public and private sector agencies should be notified on a need to know basis, particularly those who may be affected by the privacy incident, or may play a role in mitigating the potential harms. For example, a privacy incident involving financial information may warrant notification to financial institutions through the federal banking agencies and the Federal Trade Commission. In those instances, it is imperative that DHS Components and personnel avoid further unnecessary disclosure of personal information, and limit the disclosure of Sensitive PII to those with a legitimate need to know.

#### c) Other Federal Government Agencies and Congress

DHS should be prepared to respond to inquiries from other governmental agencies such as the Government Accountability Office (GAO) and Congress. The Component Head, DHS CIO, and DHS Office of Legislative Affairs will work closely to determine when notification of the incident should be provided to congressional oversight committee chairs. With respect to a major privacy incident, the DHS Office of Legislative Affairs and DHS Office of Public Affairs, with the DHS Chief Privacy Officer, will coordinate so that notification to the appropriate committee chair(s) is issued either in advance of or along with the issuance of a press release or notification to affected individuals.

Finally, it is important to ensure that any documents pertaining to the internal decision-making process (e.g., release, notification letter to affected individual(s), media release, FAQs, or other materials) can be attached to the Privacy Incident Report in the enterprise incident database.

## Closure

Once mitigation for the privacy incident is completed, the Component Privacy Officer/PPOC or the responsible SOC should update the Privacy Incident Report in the ECOP and recommend incident closure. This recommendation is subject to review by the DHS Privacy Office, Director of Privacy Incidents, and DHS CIO. However, the ultimate decision to close the incident rests with the DHS Chief Privacy Officer.

Until this determination is reached and the DHS Privacy Office, Director of Privacy Incidents, or the DHS CIO notifies the DHS SOC that incident is closed, the incident will remain open for review or further incident handling.

## Lessons Learned

The final task in the Privacy Incident Roadmap is to conduct a lessons learned exercise, when appropriate, which underscores the importance of maintaining the incident record through each activity. This documentation serves as the basis for identifying lessons learned, which can enable DHS to implement specific, preventative actions to protect and safeguard PII.

In the case of a major privacy incident, OMB requires DHS to convene the BRT to formally conduct a lessons learned exercise, and to document any findings in a supplemental report to Congress.<sup>30</sup> In the case of a minor privacy incident, the DHS Chief Privacy Officer will rely on the Component Privacy Officer/PPOC to convene a small task group to review the incident or assign the task to the Component Privacy Office incident manager, as appropriate.

The lessons learned exercise should review the incident to determine whether the root cause of the incident can be identified, such as a privacy incident of policy or procedure, a security lapse, or even malfeasance. By identifying the root cause, the Component Privacy Office can identify potential ways to enhance or strengthen employee awareness through training or awareness campaigns, as well as potential changes to policies or procedures to assist DHS personnel in safeguarding PII.

This final task, which should be documented in the enterprise incident database, is important to improving DHS's ability to prevent future privacy incidents and better safeguard PII. As part of the required reporting under FISMA, OMB requires DHS to not only document the status of each privacy incident that occurred during the fiscal year, but also to document the lessons learned OMB requires agencies to document any changes to breach response plans, policies, training, or other documentation resulting from lessons learned.

---

30. OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information."

# Conclusion

DHS personnel have important roles in supporting the Department to accomplish its mission, which is to safeguard the American people, our homeland, and our values. Every individual has a role in protecting the personal information of U.S. citizens, DHS personnel, lawful residents, visitors, and non-immigrant aliens in the custody of DHS. This responsibility begins with training and following DHS policies and procedures, and reporting suspected or confirmed privacy incidents in a timely manner.

Reporting a suspected or confirmed privacy incident in a timely manner is not only required by federal law and policy, but also helps DHS to maintain the public's trust. The PIHG is an instructional "roadmap" for handling privacy incidents, actions to be taken to resolve the incident, as well as lessons learned. The ability of DHS to successfully mitigate and prevent privacy incidents begins with the ability of DHS personnel to spot a privacy incident and the willingness to report. In fact, the first step, **reporting** a suspected or confirmed privacy incident matters the most in containing, mitigating, and resolving a privacy incident.

If you have questions about your responsibilities or specific information about who to contact within your Component regarding a suspected or confirmed privacy incident, please contact your supervisor, Component Privacy Officer/PPOC, or the DHS Privacy Office, Director of Privacy Incidents.

# Appendices

- A. Privacy Incident Contact Information – Tear Sheet for Quick Reference
- B. DHS Privacy Incident Response Process: Minor and Major Privacy Incidents
- C. DHS Headquarters Incident Intake Form
- D. Definitions
- E. Acronyms

# Appendix A: Privacy Incident Response Points of Contact (“Tear Sheet” Reference)

## SUSPECT A PRIVACY INCIDENT?

## Report, Don’t Wait!

Contact anyone  
of the following:

**your supervisor**



**your Help Desk**



**your Privacy Officer/  
PPOC**

DHS personnel have an obligation to report a suspected or confirmed breach of Personally Identifiable Information (PII) immediately



**U.S. Customs and Border Protection (CBP)**  
Help Desk  
CBP.TECHNOLOGY.SERVICE.DESK@cbp.dhs.gov  
Ph: 1-800-927-8729  
Privacy Officer: Debra Danisek  
Ph: 202-344-1610  
privacyincidents@cbp.dhs.gov

**DHS Headquarters (DHS HQ)**  
Help Desk  
ITSupport@hq.dhs.gov  
Ph: 1-800-250-7911  
Chief Privacy Officer: Sam Kaplan  
Ph: 202-343-1717  
privacyhelp@dhs.gov

**Federal Emergency Management Agency (FEMA)**  
Help Desk  
HLPFEMAFEMA-Enterprise-Service-Desk@fema.dhs.gov  
Ph: 1-888-457-3362  
Privacy Officer: William Holzerland  
Ph: 202-212-5100  
FEMA-Privacy@fema.dhs.gov

**Federal Law Enforcement Training Center (FLETC)**  
Help Desk  
Fletc-CIOITServiceDesk@dhs.gov  
Ph: 912-261-3700  
Privacy Officer: Alicia Aldridge  
Ph: 912-267-3103  
Alicia.aldridge@fletc.dhs.gov

**U.S. Immigration and Customs Enforcement (ICE)**  
Help Desk  
ICEServiceDesk@ice.dhs.gov  
Ph: 1-888-347-7762  
Privacy Officer: Amber Smith  
Information Governance and Privacy (IGP)  
Ph: 202-732-3300  
ICEPrivacy@dhs.gov

**Office of Intelligence and Analysis (I&A)**  
Help Desk  
ITSupport@hq.dhs.gov  
Ph: 1-800-250-7911  
Privacy Officer: Art Sepeta  
Ph: 202-447-3984  
Arthur.Sepeta@hq.dhs.gov

**National Protection and Programs Directorate (NPPD)**  
Help Desk  
ITSupport@hq.dhs.gov  
Ph: 1-800-250-7911  
FPS Help Desk: fps.it.support@hq.dhs.gov  
Privacy Officer: Jamie Danker  
Ph: 703-235-2182  
NPPDPrivacy@hq.dhs.gov

**Science and Technology Directorate (S&T)**  
Help Desk  
ITSupport@hq.dhs.gov  
Ph: 1-800-250-7911  
Privacy Officer: Christopher Lee  
Ph: 202-254-2341  
STPrivacy@hq.dhs.gov

**US Citizenship and Immigration Services (CIS)**  
Help Desk  
<https://dhsuscisprod.service-now.com/myIT>  
Ph: 1-888-220-5228  
Privacy Officer: Donald Hawkins  
Ph: 202-272-8404  
USCIS.PrivacyIncidentsbreaches@uscis.dhs.gov

**Transportation Security Administration (TSA)**  
Help Desk  
Email: tsaithelpdesk@tsa.dhs.gov  
Ph: 1-800-253-8571  
Privacy Officer: Peter Pietra  
TSAPrivacy@tsa.dhs.gov

**US Coast Guard (USCG)**  
Help Desk  
CGFixit@uscg.mil  
Ph: 855-243-4948  
Acting Privacy Officer: Al Craig  
Ph: 202-475-3528  
Albert.L.Craig@uscg.mil

**US Secret Services (USSS)**  
Help Desk  
ITO-ServiceDesk@uss.dha.gov.  
Ph: 202-406-5988  
Privacy Officer: Latita Payne  
Ph: 202-406-5503  
latita.payne@uss.dhs.gov

Be careful: when reporting the incident, don't duplicate or forward the PII

## Appendix B: DHS Response Process for Privacy Incidents

### Steps to Follow in Response to a Privacy Incident

*Note: incident handling should be performed in the order of priority as warranted by the circumstances of each incident. Some steps may be taken multiple times during the investigation.*

#	TASK	ASSIGNED TO	NOTES	Minor	Major
1	<p><b>Report Incident</b></p> <p>Component staff reports a suspected or confirmed incident by phone or email to Component Help Desk or Component Privacy Officer/PPOC</p>	<p>Component Staff</p> <p>System Admin</p> <p>ISSO</p>	<p>Each Component has its own email/ phone contact.</p> <p>See Appendix A</p>	X	X
2	<p><b>Intake</b></p> <p>Gather facts using Component or HQ-specific Intake Form.</p> <p>Confirm whether privacy incident has occurred.</p>	<p>Component Privacy Officer/ PPOC</p>	<p>See Appendix C, suggested sample intake form.</p>	X	X
3	<p><b>Assess and Prioritize</b></p> <ul style="list-style-type: none"> <li>Component Privacy Officer/ PPOC or SOC enters incident in the incident database and assigns a priority level within 24 hours after determining a privacy incident has occurred.</li> <li>SOC transmits privacy incident notification to Component Privacy Officer/PPOC.</li> </ul> <p>Cont.</p>	<p>Component Privacy Officer/ PPOC</p> <p>SOC</p>	<p>All SPII incidents are moderate or high.</p>	X	X

#	TASK	ASSIGNED TO	NOTES	Minor	Major
3	<p><b>Assess and Prioritize cont.</b></p> <p>If the incident is caused by a contractor, review the contract for inclusion of any privacy incident notification or incident response requirements.<sup>31</sup> All steps listed below must include collaboration between the Component Privacy Officer/PPOC and the contractor representative.</p>		DHS incorporates clauses into its contracts that define contractor responsibilities when responding to a Sensitive Information incident (see HSAR Class Deviation 15-01). <sup>32</sup> The Federal Acquisition Regulations (FAR) Council is currently drafting new government-wide FAR clauses in response to OMB issuing OMB M-17-12.		
4	<p><b>Incident-related Notifications – Minor Privacy Incident</b></p> <ul style="list-style-type: none"> <li>• SOC reports incident to US-CERT within one hour of being reported to the DHS SOC.</li> <li>• If incident involves employee financial or benefit information, PPOC notifies Component human capital office, DHS CHO and the CFO.</li> <li>• If incident impacts multiple Components, note this in the incident database and notify other Components.</li> </ul> <p>Cont.</p>	<p>Component Privacy Officer/ PPOC</p> <p>SOC</p>		X	

31. Pursuant to OMB M-17-12, “[a]gencies shall insure that contract terms necessary for the agency to respond to a breach are included in contracts when a contractor collects or maintains Federal information on behalf of the agency or uses or operates an information system on behalf of an agency.” See pp. 11-13.

32. See <https://www.dhs.gov/sites/default/files/publications/HSAR%20Class%20Deviation%2015-01%20Safeguarding%20of%20Sensitive%20Information.pdf>.

#	TASK	ASSIGNED TO	NOTES	Minor	Major
4	<p><b>Incident-related Notifications – Minor Privacy Incident cont.</b></p> <ul style="list-style-type: none"> <li>If criminal intent is found, notify senior management and law enforcement. [PPOC, SOC and responsible SOC coordinate with OCSO, OGC, and OIG]</li> <li>If the security/suitability of data is compromised, notify the OCSO.</li> </ul>				
	<p><b>Incident-related Notifications – After Escalation to a Major Privacy Incident</b></p> <p><b>Within one hour of being escalated:</b></p> <ul style="list-style-type: none"> <li>SOC to confirm US-CERT receipt of incident classification as major</li> <li>US-CERT to notify OMB</li> </ul> <p><b>Within 7 days:</b></p> <ul style="list-style-type: none"> <li>DHS Chief Privacy Officer and OLA to notify appropriate congressional committees</li> </ul> <p><b>Within 30 days:</b></p> <ul style="list-style-type: none"> <li>DHS Chief Privacy Officer to provide more details to same committees</li> </ul>	<p>DHS Chief Privacy Officer</p> <p>SOC</p> <p>US-CERT</p>	<p>See OMB M-17-12, p. 20,, for more details on reporting to Congress</p>		<p>X</p>

#	TASK	ASSIGNED TO	NOTES	Minor	Major
5	<p><b>Confirm Determination of Major or Minor Privacy Incident</b></p> <p>Confirm determine of privacy incident is either a minor or major privacy incident.</p> <p>As part of such determination, identify which system of records notice (SORN), Privacy Impact Assessment (PIA), or other compliance documents apply to the compromised PII.</p>	<p>DHS Chief Privacy Officer</p> <p>Component Privacy Officer/ PPOC</p> <p>Assistance from CIO, CISO.</p>		X	
6	<p><b>DHS Chief Privacy Officer convenes and leads the Breach Response Team (BRT)</b></p> <ul style="list-style-type: none"> <li><b>NOTE:</b> The DHS Chief Privacy Officer has the authority to escalate any privacy incident and convene the BRT within 72 hours after the DHS Chief Privacy Officer, in consultation with the CIO and CISO, has determined a Major Privacy Incident has taken place.</li> </ul> <p>Further, the DHS Chief Privacy Officer has the discretion to convene the BRT if the privacy incident is significant but does not rise to the definition of a Major Privacy Incident.</p>	<p>DHS Chief Privacy Officer</p> <p>PRIV</p> <p>BRT</p>	<p>Refer to DHS Privacy Policy Instruction 047-01-006, Privacy Incident Responsibilities and Breach Response Team.</p>		X

#	TASK	ASSIGNED TO	NOTES	Minor	Major
7	<b>Investigate</b> Initiate technical investigation to include chain of custody of PII.	Component Privacy Officer/ PPOC  SOC	Document in incident database.	<b>X</b>	
		BRT  SOC	Document in incident database.		<b>X</b>
8	<b>Risk Assessment</b> Assess the type of risk involved in the incident, and the risk of harm to the individuals impacted by a privacy incident, including: <ul style="list-style-type: none"> <li>the nature and sensitivity of the PII compromised<sup>33</sup> (e.g., data elements, context, privacy information, vulnerable populations, permanence);</li> <li>the likelihood of access and use of the PII (e.g., security safeguards, format and media, duration of exposure, evidence of misuse);</li> <li>the type of privacy incident, including the intent and the recipient(s).</li> </ul>	Component Privacy Officer/ PPOC	Refer to PIHG	<b>X</b>	
		BRT	Refer to PIHG		<b>X</b>

33. The PPOC should identify applicable privacy compliance documentation, including the responsibility to identify any applicable Privacy Act system of records notices (SORN), privacy impact assessments (PIA), and privacy notices that may apply to the potentially compromised information.

#	TASK	ASSIGNED TO	NOTES	Minor	Major
9	<p><b>Mitigation</b></p> <p>Determine appropriate mitigation steps based on the risk assessment, and document in the incident database.</p> <ul style="list-style-type: none"> <li>Component Privacy Officer/ PPOC (minor incident) or the BRT (major incident) handles non-technical mitigation.</li> <li>SOC handles technical clean up along with the Data Centers.</li> </ul> <p>Examples include:</p> <ul style="list-style-type: none"> <li>Contain/eradicate compromised PII;</li> <li>Notify affected individuals by email or mail (see OMB M-17-12, pp. 29-34);</li> <li>Offer credit monitoring/identity protection services;</li> <li>Train/counsel staff on best practices to safeguard Sensitive PII.</li> </ul>	<p>Component Privacy Officer/ PPOC</p> <p>SOC</p>	<ul style="list-style-type: none"> <li>For credit monitoring, use blanket purchase agreements (BPA) (i.e., Immigration and Customs Enforcement (ICE) and General Services Administration (GSA)).<sup>34</sup></li> </ul>	<b>X</b>	
		<p>BRT</p> <p>SOC</p>	<ul style="list-style-type: none"> <li>Refer to PIHG and 4300A, Att. F.</li> <li>Per M-17-12, DHS Secretary can delay notification in the event of a law enforcement investigation.<sup>35</sup></li> <li>After input from the BRT, the DHS Chief Privacy Officer provides recommendations for notification to the Secretary</li> </ul>		<b>X</b>

34. See, <http://dhsconnect.dhs.gov/org/comp/mgmt/cpo/oss/Documents/Strategic%20Sourcing/Department-wide-Component-wide%20Contract%20Vehicles%20-%20Currently%20In%20Place/FSSI%20Identity%20Protection%20Services/main.htm>

35. As the heads of Intelligence Community elements, so can the United States Information Agency and the USCG Commandant, as appropriate.

#	TASK	ASSIGNED TO	NOTES	Minor	Major
<b>Notification Steps for a Major Privacy Incident (9a — 10b)</b>					
9a	<p><b>Draft Statement of Work (SOW) for Vender Notification Services</b></p> <ul style="list-style-type: none"> <li>If the BRT recommends and the Secretary decides to notify impacted individuals and provide identity protection services, a Vendor must be engaged.</li> <li>ICE and GSA have a BPA with an identity protection vendor. A SOW must be drafted to engage the vendor for each privacy incident.</li> </ul> <p><u>The vendor will provide:</u></p> <ul style="list-style-type: none"> <li>18 months credit monitoring</li> <li>Address lookup/verification</li> <li>Notification and call center services</li> <li>Notification lists and reports</li> </ul>	BRT			X
9b	<p><b>Engage Vendor</b></p> <p>Once SOW is approved, call Vendor to discuss the engagement.</p>	BRT	Establish scheduled calls with Vendor regarding Call Center and Notice deliverables and performance.		X
9c	<p><b>Draft Notice</b></p> <p>Determine signatory.</p> <p>Reviewers should include: Component Privacy Officers/ PPOCs, OPA, OGC/OCC, OLA, and Vendor</p>	BRT	May request sample from Vendor or refer to other DHS examples.		X

#	TASK	ASSIGNED TO	NOTES	Minor	Major
9d	<p><b>Request Residential Address List</b></p> <p>Obtain home addresses of affected employees from Component Human Capital Office, or CSO, or from relevant system administrator if member of the public.</p> <p>Vendor will not initiate notification procedures until they receive the list of affected individuals.</p>	BRT	Obtain instructions from Vendor for secure file transfer protocols and file format specifications		X
9e	<p><b>Draft Frequently Asked Questions (FAQ)</b></p> <ul style="list-style-type: none"> <li>Prepare FAQs to accompany notice. Suggested limit of 20, and no FAQ should address identity repair.</li> </ul> <p>FAQs will accompany notice, be posted online, and used by OPA and the Call Center.</p>	BRT			X
9f	<p><b>Vendor Verifies Residential Addresses and Sets Up Call Center</b></p> <p>Vendor verifies addresses and compares against the U.S. Postal Service National Change of Address (NCOA) to ensure accuracy.</p> <p>Vendor sets up call center.</p>	Vendor			X

#	TASK	ASSIGNED TO	NOTES	Minor	Major
10	<p><b>Internal/External Communications</b></p> <ul style="list-style-type: none"> <li>• <b>Brief OPA</b> prior to sending notice and provide them with FAQs.</li> <li>• <b>Inform Congress</b> about release of notification.</li> <li>• <b>Draft a press release</b> and issue the day <u>before</u> sending the notice and <u>AFTER</u> informing OMB and Congress.</li> <li>• <b>Inform all applicable DHS union heads</b> prior to sending notice</li> </ul>	BRT	Engage OPA for assistance in drafting press release.		X
10a	<p><b>Create Webpage</b></p> <p>Set up webpage on DHS.gov as a resource for impacted individuals with:</p> <ul style="list-style-type: none"> <li>• Summary of incident</li> <li>• FAQs</li> <li>• Call center contact information</li> </ul>	BRT	Post on <a href="https://www.dhs.gov/">https://www.dhs.gov/</a> focus and link to new page. This page should go live same day as the press release.		X
10b	<p><b>Mail Notice &amp; Activate Call Center</b></p> <p>Vendor sends notification letters and the call center goes live.</p> <p>Vendor will contact BRT with referral questions and refine the call center script responses as needed.</p>	Vendor	Align activation of call center, notice, webpage, and press release.		X
11	<p><b>Close Incident in Incident Database</b></p> <p>Component Privacy Officer/PPOC sends tasking in incident database to DHS Privacy Office (PRIV) to review and close incident.</p> <p>PRIV reviews all mitigation steps and recommends closure or requests more information from Component Privacy Officer/PPOC.</p>	Component Privacy Officer/ PPOC  PRIV  SOC		X	
		PRIV  BRT  SOC			X

#	TASK	ASSIGNED TO	NOTES	Minor	Major
12	<p><b>Lessons Learned</b></p> <p>Based on incident trends, PRIV or BRT will work with Component Privacy Officer/PPOC to identify prevention steps, additional or targeted training, and/or personnel communications.</p> <p><b>NOTE:</b> In the case of a major incident, the BRT conducts the Lessons Learned exercise and includes findings in a supplemental report to Congress, as required.</p>	PRIV Component Privacy Officer/ PPOC	Document Lessons Learned in the Incident Database	<b>X</b>	
		BRT			<b>X</b>

# Appendix C: DHS Headquarters Privacy Incident Intake Form<sup>37</sup>

## Department of Homeland Security (DHS) Headquarters Privacy Incident Initial Reporting Form

This form is intended to provide information regarding the INITIAL discovery of a suspected or confirmed incident involving personally identifiable information (PII) (i.e., a "privacy incident"). DHS personnel should report a privacy incident as soon as possible and should not delay reporting due to lack of information. Additional information can be submitted as often as necessary.

DHS Incident Number: \_\_\_\_\_ Today's Date: \_\_\_\_\_  
(The assigned incident number will be provided by the DHS EOC.)

### DHS Personnel Making Initial Report

Name: \_\_\_\_\_ | Component/Office: \_\_\_\_\_

Phone Number: \_\_\_\_\_ | Email: \_\_\_\_\_

DHS employee/detailee                       Contractor                       Other

### Suspected or Confirmed Loss of PII (Privacy Incident) Information

Date of Privacy Incident: \_\_\_\_\_ | Components Affected: \_\_\_\_\_

#### Cause of Incident (pick one):

Unencrypted Email Outgoing                       Unencrypted Email Incoming  
 Lost/stolen package                       Lost/stolen equipment or mobile device  
 Other (describe): \_\_\_\_\_

#### Summary:

#### Type of PII Compromised (e.g., DOB, SSN, credit card/financial account number, medical diagnosis, address, etc.):

#### Data Storage/Collection/Media Type involved in Privacy Incident:

Paper                       Mobile Device (laptop, tablet, smartphone)  
 External Storage Device (USB, CD, DVD, other)                       IT System (server, shared drive, database, other)  
 Other (describe): \_\_\_\_\_

If the privacy incident involved paper, was it marked correctly?                       Yes     No     N/A

If the privacy incident involved email:                       Yes     No     N/A  
    A. Did the recipient have a need to know?                       Yes     No     N/A  
    C. Did the email stay within .gov domain?                       Yes     No     N/A  
    D. Was the email encrypted?                       Yes     No     N/A

#### If the privacy incident involved equipment or mobile device:

Government owned                       Contractor owned                       Personally owned  
 Encrypted                       Password protected

List any initial mitigation steps:

**Criticality:**    Minor                       Significant                       Unconfirmed/unknown

**DIRECTIONS:** Email form to [HQSOC@HQ.DHS.GOV](mailto:HQSOC@HQ.DHS.GOV)

37. The DHS Headquarters Incident Intake form contains form fields utilized by the EOC in its incident database. This form may be used or adapted by the Component Privacy Officer/PPOC.

## Appendix D: Definitions

**Access** – The ability or opportunity to gain knowledge of PII.

**Breach** – A breach is a type of incident that involves PII. There are two types of breach: intentional and unintentional. The DHS breach definition is discussed further in the “Privacy Incident” definition below. DHS changed its long standing definition of privacy incident to comport with OMB’s definition of a breach in OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of PII* (Jan. 3, 2017). However, DHS kept the term “privacy incident” to be consistent with other DHS incident types.

**Breach Response Team (BRT)** – The DHS Breach Response Team (BRT) is composed of senior Department and Component officials, or their representatives, who may be convened by the DHS Chief Privacy Officer to respond to the breach. The BRT is responsible for advising the DHS Chief Privacy Officer and the Department Leadership on effectively and efficiently responding to the breach, including conducting assessing the risk of harm to individuals, considering potential mitigations, and implementing notification for a Major Privacy Incident, as well as developing lessons learned.

**Computer Security Incident** – Violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. (NIST SP 800-61, *Computer Security Incident Handling Guide*, March 2008).

**Control** – Authority of the government agency that maintains information, or its successor in function, to regulate access to the information. Having control is a condition or state and not an event. Loss of control is also a condition or state that may or may not lead to an event (e.g., a Privacy Incident or Breach).

**DHS Personnel** – Includes federal employees, interns, detailees, independent consultants, government contractors, grantees, and others using, or with access to, DHS information.

**Federal Information** – Information created, collected, processed, disseminated, or disposed of by or for the Federal Government.

**Grantee** – A recipient of a federal award. When a grant recipient uses or operates a federal information system or creates, collects, uses, processes, stores, maintains, disseminates, discloses, or disposes of PII within the scope of a federal award, the Department shall ensure that the grant recipient has procedures in place to respond to a privacy incident.

**Harm** – Damage, fiscal damage, or loss or misuse of information that adversely affects one or more individuals or undermines the integrity of a system or program. Harms include anticipated threats or hazards to the security or integrity of records that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual whose information is maintained. The range also includes harm to reputation and the potential for harassment or prejudice, particularly when health or financial benefits information is involved.

**HSAR Clauses** – Homeland Security Acquisition Regulations. DHS published modifications to the HSAR.

The Federal Acquisition Council will soon issue standard clauses that DHS will insert in future contractor Statement of Work and Performance Work Statements.

**Incident** – An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. See 44 U.S.C. § 3552(b)(2).

**Information Resources** – Personnel, equipment, funds, and information technology. See 44 U.S.C. § 3502(6).

**Information Technology** – Any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. For purposes of this definition, such services or equipment if used by the agency directly or is used by a contractor under a contract with the agency that requires its use; or to a significant extent, its use in the performance of a service or the furnishing of a product. The term “information technology” includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources. The term “information technology” does not include any equipment that is acquired by a contractor incidental to a contract which does not require its use. See 40 U.S.C. § 11101(6).

**Major Privacy Incident** – A privacy incident that 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; and pertains to an unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to 100,000 or more individuals' PII.

**Need-to-Know** – This term refers to an exception under the Privacy Act that authorizes disclosures of Privacy Act protected records within an agency to agency staff to fulfill their job responsibilities for necessary, official agency purposes and mission needs. See 5 U.S.C. § 552a(b)(1). For disclosures not covered by the Privacy Act, access to the information must be necessary for a person to conduct his or her official duties. This is separate from whether the person has all the necessary official approvals (such as a security clearance) to access certain information.

**Personally Identifiable Information (PII)** – Any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employees or contractor to the Department.

**Privacy Incident** - The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence when (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 pur-

pose. 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” can be used synonymously with the term “breach.” The term “privacy incident” does not include or pertain to doxxing, which is described in DHS Policy Directive 121-07, “Information (also known as Sensitive Personally Identifiable Information) is Posted on the Internet and/or Social Media (Doxxing).”

**Reasonable Risk of Harm** – Likelihood that an individual may experience substantial harm, embarrassment, inconvenience, or unfairness based on information involved in a privacy incident.

**Senior Agency Official for Privacy (SAOP)** – Pursuant to OMB Memorandum M-16-24, OMB requires agencies to designate a SAOP. The Department’s designated SAOP is the DHS Chief Privacy Officer and Freedom of Information Act Officer. The SAOP advises DHS Secretary and Deputy Secretary on approaches to all privacy-related matters.

**Sensitive Information** – Any information that if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of federal programs, or the privacy of individuals, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy.

Some examples of ‘Sensitive Information’ includes:

- Chemical-terrorism Vulnerability Information (CVI)
- Protected Critical Infrastructure Information (PCII)
- Sensitive Security Information (SSI)
- Personally Identifiable Information (PII)
- Sensitive Personally Identifiable Information (SPII)

**Sensitive Personally Identifiable Information** – PII that if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII requires stricter handling guidelines because of the increased risk to an individual if the data is compromised. Some forms of PII are sensitive as stand-alone data elements. Examples of such PII include: SSN, driver’s license or state identification number, passport number, Alien Registration Number, or financial account number. Other data elements such as citizenship or immigration status; medical information; ethnic, religious, sexual orientation, or lifestyle information; and account passwords, in conjunction with the identity of an individual (directly or indirectly inferred), are also Sensitive PII. Additionally, the context of the PII may determine whether it is sensitive, such as a list of employees with poor performance ratings.

**Services** – When determining how to mitigate the risk of harm to individuals affected by a privacy incident, the SAOP shall determine if there are services the agency can provide (i.e., identity monitoring, credit monitoring, identity theft insurance, and other related services).

## Appendix E: Acronyms

<b>BRT</b>	Breach Response Team
<b>CFO</b>	Chief Financial Officer
<b>CHCO</b>	Chief Human Capital Officer
<b>CIO</b>	Chief Information Officer
<b>CISO</b>	Chief Information Security Officer
<b>CSO</b>	Chief Security Officer
<b>DHS</b>	Department of Homeland Security
<b>FIPS</b>	Federal Information Processing Standard
<b>FISMA</b>	Federal Information Security Modernization Act
<b>IP</b>	Internet Protocol
<b>IT</b>	Information Technology
<b>NIST</b>	National Institute of Standards and Technology
<b>OCC</b>	Office of Chief Counsel
<b>OGC</b>	Office of the General Counsel
<b>OIG</b>	Office of Inspector General
<b>OMB</b>	Office of Management and Budget
<b>OPM</b>	Office of Personnel Management
<b>PIHG</b>	Privacy Incident Handling Guidance
<b>PIA</b>	Privacy Impact Assessment
<b>PII</b>	Personally Identifiable Information
<b>PIN</b>	Personal Identification Number
<b>PM</b>	Program Manager
<b>PPOC</b>	Privacy Point of Contact
<b>PTA</b>	Privacy Threshold Analysis
<b>SAOP</b>	Senior Agency Official for Privacy
<b>SOC</b>	Security Operations Center
<b>SPII</b>	Sensitive Personally Identifiable Information
<b>SSN</b>	Social Security number
<b>U.S.C.</b>	United States Code
<b>US-CERT</b>	United States Computer Emergency Readiness Team