Privacy Incident Handling Guidance

Revised January 26, 2012

Homeland Security

Basis for Privacy Incident Handling Guidance

The following procedures establish governing policies and procedures for Privacy Incident handling at the Department of Homeland Security (DHS). The policies and procedures are based on applicable laws, Presidential Directives, and Office of Management and Budget (OMB) directives.

Please contact the DHS Privacy Office at privacy@dhs.gov or 703-235-0780 concerning questions about Privacy Incident handling or this Guidance.

TABLE OF CONTENTS

1. Introduction

1.1. Purpose

The Department of Homeland Security (DHS) has a duty to safeguard personally identifiable information (PII) in its possession, and to prevent the compromise of PII in order to maintain the public's trust in DHS. The Privacy Incident Handling Guidance (PIHG) serves this purpose by informing DHS and its components, employees, senior officials, and contractors of their obligation to protect PII, and by establishing procedures defining how they must respond to a privacy incident, which is the potential loss or compromise of PII. The PIHG also creates individual accountability for compliance.

The PIHG establishes DHS policy and procedures for DHS personnel to follow upon the detection or discovery of a suspected or confirmed incident involving PII. DHS defines PII as 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 United States citizen, legal permanent resident, or a visitor to the U.S. *See Appendix C for Illustrations of Privacy Incidents.*

The Office and Management and Budget (OMB) requires agencies to report all Privacy Incidents to the United States Computer Emergency Readiness Team (US-CERT) within one hour of discovering the incident, as mandated by OMB Memorandum M-06-19 (OMB M-06-19), *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 12, 2006, and OMB Memorandum M-07-16 (OMB M-07-16), *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007. The one hour time requirement begins when the DHS Chief Information Security Officer (DHS CISO) is notified of the incident.

OMB M-07-16 further defines the appropriate reporting, handling, and notification procedures in the event a Privacy Incident occurs. It establishes two strict reporting timelines. First, OMB M-07-16 mandates that personnel report a Privacy Incident as soon as possible. OMB M-07-16 also requires the Department to report the Privacy Incident to US-CERT within one hour. The memorandum also clarifies that PII and information systems containing such information should generally be categorized as either Moderate-Impact or High-Impact for implementing minimum baseline security requirements and controls. See Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems* for additional information. Finally, it recommends minimum requirements for agency policies detailing the responsibilities of individuals authorized to access PII.

1.2. Scope

The PIHG applies to all DHS personnel, including contractors, and to all federal information and information systems in an unclassified environment, and includes information in any format (e.g., paper, electronic, etc.). Although most incidents involve information technology, a Privacy

Incident may also involve physical security considerations that may cause the compromise of PII.

If a Privacy Incident impacts the security of an information technology (IT) system, DHS personnel must refer to the DHS Concept of Operations (CONOPS) for Security Operations Centers (SOC).

For guidance on Privacy Incident handling of federal information in a classified environment, refer to *DHS 4300B National Security Systems Handbook*.

1.3. 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. Additional federal statutes, regulations, and directives are located in Appendix B.

- The Privacy Act of 1974, 5 U.S.C. § 552a, provides privacy protections for records containing information about individuals (i.e., citizen and legal permanent resident) that are collected and maintained by the federal government and are retrieved by a personal identifier. The Act requires agencies to safeguard information contained in a system of records.
- Section 222 of the Homeland Security Act of 2002 (Public Law 107-296, 6 U.S.C. § 142) mandates that the Secretary of DHS appoint a senior official in the Department to assume primary responsibility for privacy policy.
- OMB Memorandum M-06-15 (M-06-15), *Safeguarding Personally Identifiable Information* (May 22, 2006) reiterates and emphasizes agency responsibilities under law and policy to appropriately safeguard sensitive PII and train employees regarding their responsibilities for protecting privacy.
- OMB Memorandum M-06-16 (M-06-16), *Protection of Sensitive Agency Information* (June 23, 2006) requires agencies to implement encryption protections for PII being transported and/or stored offsite.
- OMB Memorandum M-06-19 (M-06-19), *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments* (July 12, 2006) requires agencies to report all incidents involving PII to US-CERT within one hour of discovery of the incident.
- OMB's Memorandum *Recommendations for Identity Theft Related Data Breach Notification* (September 20, 2006) outlines recommendations to agencies from the President's Identity Theft Task Force for developing agency planning and response procedures for addressing PII incidents that could result in identify theft.
- OMB Memorandum M-07-16 (M-07-16), *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007) identifies existing

procedures and establishes several new actions agencies should take to safeguard PII and to respond to Privacy Incidents.

1.4. Definitions

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

1.4.2. 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).

1.4.3. 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 which may or may not lead to an event (e.g., a Privacy Incident).

1.4.4. DHS Personnel – Includes federal employees, independent consultants, government contractors and others using, or with access to, DHS information resources.

1.4.5. Federal Information – Information created, collected, processed, disseminated, or disposed of by or for the federal government.

1.4.6. 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 which 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**.**

1.4.7. Information Resources – Information and related resources, such as personnel, equipment, funds, and information technology. This term includes both government information and technology. (NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003; OMB Circular A-130(6)(n), *Management of Federal Information Resources*, November 28, 2000).

1.4.8. Information Technology – Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. Equipment refers to that used by any DHS Component or contractor, if the contractor requires the use of such equipment in the performance of a service or the furnishing of a product in support of DHS. The term "information technology" includes computers, ancillary equipment, software, firmware

and similar procedures, services (including support services), and related resources (40 U.S.C. § 11101). The term "information technology" does not include national security systems as defined in the Clinger-Cohen Act of 1996 (40 U.S.C. § 11103) and OMB Circular A-130. The term "information system" used in this document is equivalent to "IT system."

1.4.9. Personally Identifiable Information (PII) – 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, legal permanent resident, or a visitor to the U.S. PII includes any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history.

Examples of PII include: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers (e.g., fingerprints), photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual. *See Privacy Impact Assessments, The Privacy Office Official Guidance*, June 2010.

1.4.10. Privacy Incident – The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, have access or potential access to PII in usable form, whether physical or electronic, or where authorized users access PII for an unauthorized purpose. The term encompasses both **suspected and confirmed incidents** involving PII which raise a reasonable risk of harm (see section 1.4.12).

1.4.11. Privacy Incident Response Team (PIRT) – A group of DHS officials at the Departmental or Component level responsible for handling Privacy Incident investigation, mitigation, and notification, with oversight by the DHS Privacy Office, Director of Privacy Incidents and Inquiries. The team includes officials responsible for administering operational, privacy, and security programs. Its membership includes legal counsel, the inspector general, law enforcement, and public and legislative affairs. Each PIRT member provides assistance with incident handling based on their capability, expertise, and authority as needed. Each office or member at the Departmental level will consult with its counterpart at the Component level to ensure consistency in the implementation of the PIHG throughout the Department. See OMB M-07-16 and OMB's Memorandum entitled, *Recommendations for Identity Theft Related Data Breach Notification*, September 20, 2006.

A PIRT may be comprised of representatives from the following offices as warranted by circumstances. These offices also comprise the Core Management Group:

- DHS Deputy Secretary
- DHS Chief Privacy Officer (CPO)
- DHS Privacy Office, Director of Privacy Incidents and Inquiries
- DHS Chief Information Officer (CIO)
- DHS Chief Information Security Officer (CISO)
- DHS Office of General Counsel (OGC)
- DHS Office of Inspector General (OIG)
- DHS Chief Security Officer (CSO)
- DHS Public Affairs Office
- DHS Legislative Affairs Office
- DHS Office of Intergovernmental Affairs
- Management Directorate
- DHS Chief Financial Officer (CFO)
- DHS Office of Health Affairs
- Component Head or designee(s)
- 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
- Component CFO

1.4.12. Reasonable Risk of Harm – Likelihood that an individual may experience substantial harm, embarrassment, inconvenience, or unfairness based on information maintained.

1.4.13. Sensitive Personally Identifiable Information – Personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. 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.

2. Roles and Responsibilities for Privacy Incident Handling

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 paper and electronic formats. DHS components and personnel must understand and adhere to all relevant federal laws, regulations, and directives, and to Departmental directives and guidance.

2.1. DHS Personnel

Privacy Incident handling responsibilities are to:

- Complete annual Privacy Awareness Training and Education.
- Recognize Privacy Incidents.
- Inform the PM of the detection or discovery of suspected or confirmed incidents involving PII; or if the PM is unavailable or has a conflict of interest, contact the Help Desk or the Privacy Officer/PPOC for the Component.

2.2. Program Manager

Privacy Incident handling responsibilities are to:

- Ensure compliance with federal laws and Departmental privacy policy concerning the operation and maintenance of information systems and programs.
- Recognize Privacy Incidents.
- Understand the Privacy Incident reporting process and procedures for the Component.
- Receive initial reports from DHS personnel regarding the possible detection of Privacy Incidents.
- Consult with the Component Privacy Officer/PPOC or Component ISSM to obtain guidance concerning Privacy Incident handling and other privacy issues affecting information systems.

- Determine whether a suspected or confirmed incident involving PII may have occurred.
- Provide a brief Preliminary Written Report to the Component IT Security Entity (e.g., Component ISSM, Component SOC, or Component CSIRC); or if the Component IT Security Entity is not available, contact the DHS SOC directly.
- Assist the Component Privacy Officer/PPOC and the Component IT Security Entity with the development of facts for the Privacy Incident Report.
- Provide advice, expertise, and assistance to the PIRT as needed.
- Assist with the investigation and mitigation of a Privacy Incident.

2.3. Component Help Desk

Privacy Incident handling responsibilities are to:

- Recognize Privacy Incidents.
- Understand the Privacy Incident reporting process and procedures.
- Serve as an alternate to the PM to receive initial Privacy Incident reports from DHS personnel when the PM is unavailable to receive the initial report or has a conflict of interest in handling the report.
- Make a brief preliminary Privacy Written Report to the Component IT Security Entity (e.g., Component ISSM, Component SOC, Component CSIRC); or if none is available, contact the DHS SOC directly.

2.4. Component Privacy Officer and Privacy Point of Contact

Privacy Incident handling responsibilities are to:

- Ensure compliance with federal laws and Departmental policy concerning safeguarding PII in consultation with the DHS CPO and Component CIO.
- Implement annual Privacy Awareness Training and Education under the direction of the DHS CPO.
- Understand and implement the Privacy Incident handling process and procedures for the Component.
- Work closely with the Component IT Security Entity, PM, DHS CPO, and DHS Privacy Office, Director of Privacy Incidents and Inquiries, regarding Privacy Incident handling and other privacy issues affecting information technology systems.
- Work with the Component IT Security Entity and the PM to ensure a complete and accurate Privacy Incident Report.
- Notify and update the DHS Privacy Office, Director of Privacy Incidents and Inquiries, of the status of a potential or confirmed Privacy Incident when needed (e.g., particularly sensitive issues, multiple component issues).

- Notify other Component Privacy Officers/PPOCs immediately upon discovery of Privacy Incidents that involve the compromise of the other Component's information, and establish who will take the lead on the Privacy Incident handling. Notification can occur through the use of conference calls, emails, and other methods.
- Consult with the Component CIO concerning Privacy Incident handling.
- Work with the Component IT Security Entity to mitigate the Privacy Incident.
- Notify the DHS CFO and Component CFO of any Privacy Incident that involves government-issued credit cards and other CFO Designated Financial Systems.
- Respond to inquiries from US-CERT regarding Privacy Incident reports, and supplement the Privacy Incident Report in the DHS EOC Online Incident Handling System as further information is obtained.
- Consult with DHS OIG as necessary.
- Assess the likely risk of harm posed by the Privacy Incident (e.g., low, moderate, or high impact) to determine who should handle the investigation, notification, and mitigation of the incident.
- Handle the investigation, notification, and mitigation for all Privacy Incidents in collaboration with the Component IT Security Entity as needed.
- Serve as a member of the PIRT if convened.
- Compose documents (e.g., notification letters) as needed.
- Coordinate joint decision with the Component Head regarding the appropriateness of external notification to affected third parties, and the issuance of a press release in Low- and Moderate-Impact Privacy Incidents that occur at the Component level.
- Provide internal notification to DHS components and senior officials as required by the PIHG prior to the authorized public release of information related to a Privacy Incident.
- Ensure incident closure recommendations are coordinated with the Component IT Security Entity and the DHS SOC.
- Maintain and update Component POC information for Privacy Incident handling.
- Provide input for the Core Management Group Privacy Incident After Action Report to the DHS Privacy Office, Director of Privacy Incidents and Inquiries.

2.5. Component IT Security Entity (e.g., Component ISSM, Component SOC, Component CSIRC)

Privacy Incident handling responsibilities are to:

- Ensure that the DHS Information Security Program is implemented and maintained throughout the Component.
- Consult and coordinate with the PM and the Component Privacy Officer/PPOC regarding privacy issues affecting the security of information.

- Understand Privacy Incident handling process and procedures.
- Consult with the Component Privacy Officer/PPOC and the PM in preparing the Privacy Incident Report in the EOC Online Incident Handling System for review by DHS SOC.
- Work with the Component Privacy Officer/PPOC to investigate and remediate aspects of Privacy Incidents that impact computer security.
- Provide advice, expertise, and assistance to PIRT as needed.
- Provide Privacy Incident closure recommendations as necessary.

2.6. DHS Security Operations Center

Privacy Incident Handling responsibilities are to:

- Serve as a central repository and coordination point for Privacy Incidents within DHS SOC.
- Maintain the ability to respond to incidents 24 hours a day, 7 days a week, and maintain a dedicated teleconference line to provide rapid scalable access.
- Provide security monitoring and analysis support, including initiation of incident handling efforts.
- Evaluate the Privacy Incident Report for sufficiency.
- Open a Privacy Incident Report for the Component when the Component Privacy Officer/PPOC or Component IT Security Entity is unavailable.
- Understand the Privacy Incident handling process and procedures.
- Transmit Privacy Incident Reports to US-CERT within one hour of receipt from the Component Privacy Officer/PPOC or Component IT Security Entity.
- Inform DHS senior officials of matters concerning Privacy Incidents through the use of automated Privacy Incident Notifications, conference calls, reports, and other methods.
- Assist DHS senior officials, Component Privacy Officer/PPOCs, and the Component IT Security Entity as needed to facilitate Privacy Incident reporting, investigation, mitigation, and incident closure.
- Provide technical assistance, share security advisories with Components, and facilitate sharing of information.

2.7. US-CERT

Privacy Incident handling responsibilities are to:

- Serve as the designated central reporting organization and repository within the federal government for federal incident data.

- Communicate and coordinate with the Component Privacy Officer/PPOC to obtain updates regarding Privacy Incident Reports.
- Notify appropriate authorities of the Privacy Incident.

2.8. DHS Chief Privacy Officer

Privacy Incident handling responsibilities are to:

- Ensure Departmental compliance with privacy policy, including, but not limited to, measures securing information security assets and activities.
- Serve as the senior DHS official responsible for oversight of Privacy Incident management.
- Establish and implement DHS privacy policy and procedures in accordance with federal laws, regulations, and policies.
- Understand the Privacy Incident handling process and procedures.
- Consult with DHS senior officials and the Component Privacy Officer/PPOC regarding Privacy Incidents as needed.
- Provide advice, expertise, and assistance to the PIRT, when necessary, in the handling of Privacy Incidents.
- Develop and implement Privacy Awareness Training and Education in coordination with the Component Privacy Officer/PPOCs.
- Provide recommendations to the PIRT and the Component Head as needed regarding the issuance of external notification to affected third parties and a press release.
- Determine who will handle non-media-related inquiries concerning the status of Privacy Incidents or the implementation of this guidance.
- Consult and coordinate with the DHS Legislative and Inter-Governmental Affairs Office to determine when notification of a Privacy Incident to the congressional oversight committee Chair is necessary.
- Examine monthly reports issued by US-CERT addressing the Privacy Incidents that were reported to US-CERT.
- Chair the Core Management Group Annual Meeting

2.9. DHS Privacy Office, Director of Privacy Incidents and Inquiries

Privacy Incident handling responsibilities are to:

- Develop, update, and maintain DHS Privacy Incident handling procedures.
- Review all incidents for accuracy and completeness, and determine whether escalation is needed to Department leadership.

- Work with the Component Privacy Officer/PPOC to ensure the incidents are properly reported, investigated and mitigated.
- Ensure all incidents that affect multiple components are properly reported, and work with the Component Privacy Officers/PPOCs to ensure they are aware of their respective roles and responsibilities in the mitigation of these incidents. Notification should occur immediately through the use of conference calls, emails, and other methods.
- Review incident closure recommendations.
- Coordinate with DHS SOC regarding the online Privacy Incident reporting system, and monitor the system to provide suggested improvements to make it more efficient and effective.
- Host quarterly Privacy Incident Handling meetings for all Component Privacy Officers/PPOCs and SOC Management Staff.
- Provide program metrics and updates to the Chief Privacy Officer for the Core Management Group annual meeting for the review of the PIHG.
- Prepare the Annual Report for the PIHG Program Review, known as the Core Management Group Privacy Incident After Action Report.

2.10. DHS Chief Information Officer

Privacy Incident handling responsibilities are to:

- Provide management direction for the DHS SOC and overall direction for the Component SOCs.
- Develop and maintain an agency-wide information security program.
- Develop and maintain information security policies, procedures, and control techniques.
- Ensure compliance with applicable information security requirements.
- Report annually, in coordination with the other senior agency officials, to the agency head on the effectiveness of the agency information security program.
- Understand the Privacy Incident handling process and procedures.
- Serve on the PIRT as needed.
- Provide recommendations to the PIRT and the Component Head as needed regarding the issuance of external notification to affected third parties and a press release.
- Consult and coordinate with the DHS Legislative and Inter-Governmental Affairs Office to determine when notification of a Privacy Incident to the congressional oversight committee Chair is necessary.

2.11. Component Chief Information Officer

Privacy Incident handling responsibilities are to:

- Provide management direction for security operations.
- Serve as an advocate for privacy and computer security incident response activities in consultation with the DHS CIO, DHS CPO, and the Component Privacy Officer/PPOC.
- Understand the Privacy Incident handling process and procedures.
- Serve on the PIRT for the Component as needed.
- Advise the DHS CIO of any issues arising from Privacy Incidents that affect infrastructure protection, vulnerabilities, or issues that may cause public concern or loss of credibility.
- Ensure that incidents are reported to the DHS SOC within the reporting time requirements as defined by the PIHG and DHS MD 4300A, Attachment F.
- Provide recommendations to the PIRT and the Component Head as needed regarding the issuance of external notification to affected third parties and a press release.

2.12. DHS Chief Information Security Officer

Privacy Incident handling responsibilities are to:

- Provide security oversight and information assurance for all DHS information systems and networks.
- Understand current issues that impact availability, confidentiality, and integrity of the network assets.
- Maintain awareness of security incidents or privacy incident reports.
- Understand the Privacy Incident handling process and procedures.
- Brief the DHS CIO and senior management on the status and outcome of ongoing and completed Computer Security Incidents.
- Assess the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of DHS information and information systems.
- Develop and maintain risk-based information security policies and procedures.
- Facilitate development of Component plans for providing adequate information security.
- Ensure that agency personnel and contractors receive appropriate information security awareness training.
- Periodically test and evaluate the effectiveness of information security policies, procedures, and practices.

- Establish and maintain processes for planning, implementing, evaluating, and documenting corrective actions to address any deficiencies in the Department's information security policies, procedures, and practices.
- Develop and implement procedures for detecting, reporting, and responding to Computer Security Incidents.
- Ensure preparation and maintenance of plans and procedures to provide continuity of operations for information systems.
- Examine monthly reports issued by US-CERT addressing Privacy Incidents that were reported to US-CERT.

2.13. Privacy Incident Response Team

Privacy Incident handling responsibilities are to:

- Understand the Privacy Incident handling process and procedures.
- Provide advice and assistance to the Component Privacy Officers/PPOCs and DHS Privacy Office, Director of Privacy Incidents and Inquiries, regarding investigation, notification, and mitigation of Privacy Incidents as needed.
- Coordinate with external entities such as law enforcement, Social Security Administration (SSA), and the Executive Office of the President (EOP) during the investigation, notification, or mitigation stages as needed.
- Provide recommendations to the Component Head regarding the issuance of external notification to affected third parties and a press release.
- Review Departmental implementation of this guidance at least annually or whenever there is a material change in Departmental practices in light of the mandates of the Privacy Act.

2.14. Heads of Components

Privacy Incident handling responsibilities are to:

- Understand the Privacy Incident handling process and procedures.
- Provide necessary resources or assistance to facilitate Privacy Incident handling.
- Provide advice, expertise, and assistance to the PIRT as needed.
- Make joint decision with the PIRT regarding the issuance of external notification to affected third parties and a press release.
- Initiate and evaluate corrective and disciplinary action when Computer Security or Privacy Incidents and violations occur.

2.15. DHS Office of the Inspector General

Privacy Incident handling responsibilities are to:

- Understand the Privacy Incident handling process and procedures.
- Consult with the Component Privacy Officer/PPOC on a case-by-case basis to determine the appropriate incident handling procedures for Moderate- and High-Impact Privacy Incidents as needed.
- Provide advice, expertise, and assistance to the PIRT when necessary, and handle Privacy Incidents in consultation with other members of the team.
- Provide recommendations to the PIRT and the Component Head as needed regarding the issuance of external notification to affected third parties and a press release.

2.16. DHS Office of the General Counsel and Component Office of the Chief Counsel

Privacy Incident handling responsibilities are to:

- Understand the Privacy Incident handling process and procedures.
- Provide advice, expertise, and assistance to PIRT, when necessary, and handle Privacy Incidents in consultation with other members of the team.
- Provide legal advice to the DHS CPO, DHS CIO, Component Privacy Officer/PPOC, Employee Relations, and supervisors regarding the potential for disciplinary or corrective action against DHS personnel arising from a Privacy Incident.
- Provide recommendations to the PIRT and the Component Head as needed regarding the issuance of external notification to affected third parties and a press release.
- Advise the Chief Human Capital Officer (CHCO) regarding disciplinary actions taken as needed.
- Review, revise, and comment on reports and corrective actions taken.

2.17. DHS Public Affairs Office and Public Affairs Office for the Component

Privacy Incident handling responsibilities are to:

- Understand the Privacy Incident handling process and procedures.
- Work with the Component Head and the PIRT to coordinate the external notification to affected third parties, and the issuance of a press release.
- Serve as sole POC for media-related inquiries about Privacy Incidents.

2.18. DHS Legislative and Inter-Governmental Affairs Office and Legislative Affairs Office for the Component

Privacy Incident handling responsibilities are to:

- Understand the Privacy Incident handling process and procedures.
- Consult and coordinate with the DHS CPO and DHS CIO to determine when notification of a Privacy Incident to the congressional oversight committee Chair is necessary.
- Provide recommendations to the PIRT and the Component Head as needed regarding the issuance of external notification to affected third parties and a press release.

2.19. DHS Management Office and Management Staff for the Component

Privacy Incident handling responsibilities are to:

- Understand the Privacy Incident handling process and procedures.
- Provide recommendations to the PIRT and the Component Head as needed regarding the issuance of external notification to affected third parties and a press release.

2.20. Chief Human Capital Officer

Privacy Incident handling responsibilities are to:

- Understand the Privacy Incident handling process and procedures.
- Work with the DHS CFO, Component Privacy Officer/PPOC, or the PIRT as needed when Privacy Incidents involve individuals' bank account numbers used for direct deposit of credit card reimbursements, government employee salaries, or any benefit information.
- Consult with the Component Head or designee(s), including Component OCC, in cases involving potential disciplinary or corrective action arising from a Privacy Incident.
- Maintain a record of all disciplinary or corrective actions taken against DHS personnel that arise out of a Privacy Incident.

2.21. DHS Chief Security Officer

Privacy Incident handling responsibilities are to:

- Provide support, guidance, and when appropriate, assistance on security related matters.
- Advise the DHS Secretary, through the Under Secretary for Management, on security-related issues affecting DHS personnel, information technology and communication systems, property, facilities, equipment, information, and other material resources.

- Provide support and guidance, and coordinates with the DHS CIO to ensure DHS IT systems are properly secured.
- Understand the Privacy Incident handling process and procedures.
- Provide advice, expertise, and assistance to the PIRT with respect to Privacy Incidents that raise security-related issues affecting personnel, property, facilities, and information.

2.22. Component Chief Security Officer

Privacy Incident handling responsibility is to:

- Understand the Privacy Incident handling process and procedures.
- Receive notification about a Privacy Incident from the PM to support and coordinate the component's response and any notifications to the DHS CSO as necessary.
- Handle external notification to law enforcement when the Privacy Incident arises from criminal activity that impacts physical security.

2.23. DHS and Component Chief Financial Officers

Privacy Incident handling responsibilities are to:

- Understand the Privacy Incident handling process and procedures.
- Coordinate with the Component Privacy Officer/PPOC when the Privacy Incident involves government-issued credit cards.
- Notify the issuing bank when the Privacy Incident involves government-issued credit cards.
- Notify the bank or other entity involved when the Privacy Incident involves individuals' bank account numbers used for direct deposit of credit card reimbursements, government salaries, travel vouchers, or any benefit payment.
- Serve as a member of the PIRT when CFO Designated Financial Systems are involved in the Privacy Incident.
- Provide recommendations to the PIRT and the Component Head as needed regarding the issuance of notification to affected third parties and a press release for Privacy Incidents involving CFO Designated Financial Systems.

2.24. DHS Deputy Secretary

Privacy Incident handling responsibilities are to:

- Ensure that DHS personnel and components understand and comply with all relevant federal laws, regulations, and directives, and Departmental regulations, policies, and guidance.

- Understand the Privacy Incident handling process and procedures.
- Consult with DHS senior officials regarding the handling of Privacy Incidents as needed.
- Provide recommendations to the PIRT and the Component Head as needed regarding the issuance of external notification to affected third parties and a press release.

2.25. DHS Secretary

Privacy Incident handling responsibilities are to:

- Ensure that DHS Personnel and components understand and comply with all relevant federal laws, regulations, and directives, and Departmental regulations and guidance.
- Understand the Privacy Incident handling process and procedures.
- Consult with DHS senior officials regarding Privacy Incidents as necessary.

3. Overview of Privacy Incident Handling Procedures

The PIHG establishes the framework for identifying, reporting, and responding to Privacy Incidents in a timely and meaningful manner. A quick and effective response in the event of a Privacy Incident is critical to prevent or minimize any consequential harm. An effective response necessitates disclosure of information about the incident to individuals affected by it, as well as to persons and entities in a position to notify affected individuals or assist in preventing or minimizing harms from the incident. Internal notifications and access to information must be limited to those who have a legitimate need to know. *See Appendix D, DHS Privacy Playbook: Handling Process Overview,* for an overview of the incident handling process.

DHS must be able to respond in a manner that not only protects its own information, but also helps 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. The strict reporting standards and timelines must be followed.

There are six stages of incident handling: (1) Reporting; (2) Escalation; (3) Investigation; (4) Notification; (5) Mitigation; and (6) Closure. The organizational structure for incident handling is designed to restrict the number of reporting tiers to the minimum necessary, while ensuring that officials responsible for safeguarding PII are fully informed of the incident.

Incident handling for the various stages must be performed in the order of priority as warranted by the circumstances. The order of the incident handling stages will differ from one incident to another.

DHS personnel including employees and senior officials must use their best judgment in executing their incident handling responsibilities. DHS personnel must act on an informed basis

in good faith and in the best interests of the agency and the individuals affected by the Privacy Incident.

DHS personnel and components must also refer to the DHS CONOPS if a Privacy Incident also impacts the security of an IT system. In this instance, both the PIHG and the CONOPS would govern incident handling because the incident would constitute both a Privacy Incident and a Computer Security Incident.

4. Reporting Procedures

4.1. Reporting Standard

DHS personnel must inform their PM immediately upon discovery or detection of a Privacy Incident, regardless of the manner in which it occurred. *See Appendix D, DHS Privacy Playbook: Handling Process Overview*, for an overview and checklist for the incident reporting process. A Privacy Incident is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users have access or potential access to PII in usable form, whether physical or electronic, or where authorized users access PII for an unauthorized purpose. The term encompasses both **suspected and confirmed incidents** involving PII that raise a reasonable risk of harm (see section 1.4.12).

DHS uses a best judgment standard in implementing the reporting requirements. Using a best judgment standard, discarding a document with the author's name on the front and no other PII into an office trash would likely not trigger the reporting requirements. Therefore, DHS personnel would not be required to report the situation because there is no reasonable risk of harm to the individual. However, a list of names (e.g., a list of FEMA beneficiaries) may result in a MODERATE or HIGH impact approach to incident response because of the identification of Sensitive PII. Sensitive PII results in a reasonably high risk of harm to the individual due to the sensitivity of the specific data elements.

4.2. No Electronic/Paper Incident Distinction

A Privacy Incident must be reported whether the PII is in electronic or physical form.

4.3. Factual Foundation for the Report

4.3.1. Initial Report

As soon as DHS personnel discover or detect a Privacy Incident, it is their duty to report the incident to the PM. If the PM is unavailable or has a conflict of interest, then DHS personnel may report the incident to the Component Help Desk. If a Component does not use the Help Desk for purposes of incident reporting, DHS personnel may report the Privacy Incident directly

to the Component Privacy Officer/PPOC or the Component IT Security Entity (e.g., Component ISSM, Component SOC, Component CSIRC).

4.3.2. Preliminary Written Report

The PM or the Help Desk for the Component must immediately make a Preliminary Written Report. At a minimum, the PM or the Help Desk must provide the Component Privacy Officer/PPOC or the Component IT Security Entity with the following information:

- Component name in which the incident occurred
- Name, phone number, and email address of the individual who discovered the incident
- Date and time of the incident and a brief description of the circumstances surrounding the potential loss of PII, including the following:
  - Summary of the type of PII potentially at risk (e.g., explain that an individual's full name, SSN, birth date, etc., may have been compromised but do not disclose specific PII in the report). Refer to the definition of PII for additional examples in Section 1.4
  - Number of people who potentially received the PII and the estimate or actual number of records exposed
  - Whether it was disclosed internally within DHS, externally, or both
  - If external disclosure is involved, state to whom it was disclosed (e.g., public website, personal email address, other government entity)
  - If applicable, whether the individual(s) had a legitimate need to know the information.

If the Component IT Security Entity, PM, or Help Desk is not available to handle reporting for the incident, or has a conflict of interest, the report may be sent directly to DHS SOC for Privacy Incident reporting.

4.3.3. Privacy Incident Report in the DHS EOC Online Incident Handling System

Upon receipt of the Preliminary Written Report, the Component Privacy Officer/PPOC and the Component IT Security Entity (e.g., Component ISSM, Component SOC, or Component CSIRC) should immediately consult and evaluate the incident. If the facts contained in the Preliminary Written Report support the conclusion that a Privacy Incident ***may have occurred***, then the Component Privacy Officer/PPOC or the Component IT Security Entity must open an incident report in the DHS EOC Online Incident Handling System at https://eoconline.dhs.gov. The Component Privacy Officer/PPOC or the Component IT Security Entity has the responsibility to open and prepare the Privacy Incident Report.

Although the Component should not delay reporting in order to gain additional information, the report should contain as much of the following information as possible, **if applicable, and to the extent the information is immediately available**:

- System name

- Component name in which the incident occurred
- System owner POC, DHS phone number, and DHS email address
- Name, phone number, and email address of the individual who discovered the incident
- Incident category type — Privacy Incidents are generally categorized as: Alteration/Compromise of Information, Misuse, Unauthorized Access, and Malicious Logic and will be prioritized based on the nature and severity of the incident
- Date and time of incident, and a brief description of the circumstances surrounding the potential loss of PII, including:
    - Summary of the type of PII that is potentially at risk (e.g., explain that an individual's full name, SSN, birth date, etc., may have been compromised, but do not disclose specific PII in the report). Refer to the definition PII for additional examples in Section 1.4
    - Interconnectivity of the system to other systems
    - Whether the incident is either suspected or confirmed
    - How PII was disclosed (e.g., email attachment, hard copy, stolen or misplaced laptop, etc.)
    - To whom it was disclosed and if the individual(s) had a legitimate need to know the information
    - Whether it was disclosed internally, within DHS
    - Whether it was disclosed externally
    - Whether it was disclosed both internally and externally
    - If external disclosure is involved, state to whom it was disclosed (e.g., public website, personal email address, other government entity)
    - Risk of the PII being misused expressed in terms of impact and likelihood
    - Security controls used to protect the information (e.g., password-protected, encryption)
    - Steps that have already been taken to reduce the risk of harm
    - Any additional steps that may be taken to mitigate the situation

4.4. Means of Reporting and Related Communications

A Privacy Incident may be reported by the Component via telephone, email, or through the DHS SOC web site (www.eoconline.dhs.gov).

Once a Privacy Incident Report has been opened in the DHS EOC Online Incident Handling System, factual updates and subsequent communications concerning any aspect of incident handling should be entered into the Privacy Incident Report to the extent possible.

4.5. Organizational Structure for Reporting a Privacy Incident within DHS

All Privacy Incidents must be reported in accordance with this Section. Diagram A provides an overview of the internal Privacy Incident reporting process.

4.5.1. Tier 1 (DHS Personnel)

Upon discovery or detection of a potential Privacy Incident, DHS personnel are responsible for immediately reporting the incident to the PM or to the Help Desk for the Component. If the PM or Help Desk is unavailable, DHS personnel may report the incident directly to the Component IT Security Entity or Component Privacy Officer/PPOC.

4.5.2. Tier 2 (PM or Help Desk)

The PM or the Help Desk for the Component will evaluate the incident with assistance from Component Privacy Officer/PPOC for the Component in which the incident occurred. The PM or the Help Desk for the Component will make a Preliminary Written Report to the Component IT Security Entity, if available. If the Component IT Security Entity is not available to handle reporting for the incident, the report may be provided to the DHS SOC.

4.5.3. Tier 3 (Component Privacy Officer/PPOC or Component IT Security Entity, or alternately DHS SOC)

The Component Privacy Officer/PPOC and the Component IT Security Entity (e.g., Component ISSM, Component SOC, or Component CSIRC) must immediately consult and evaluate the factual basis of the incident. The Component Privacy Officer/PPOC and the Component IT Security Entity must develop the factual basis for an accurate and complete report.

The circumstances surrounding the incident will determine whether the Component Privacy Officer/PPOC or the Component IT Security Entity opens, prepares, and submits the Privacy Incident report of the incident in the DHS EOC Online Incident Handling System. If the Component IT Security Entity is unavailable, the DHS SOC will prepare and submit the report to meet the strict Privacy Incident reporting time requirements.

4.5.4. Tier 4 (DHS SOC)

The DHS SOC will review the Privacy Incident Report for factual sufficiency and transmit the report to US-CERT within one hour of receiving the Privacy Incident Report from the Component IT Security Entity.

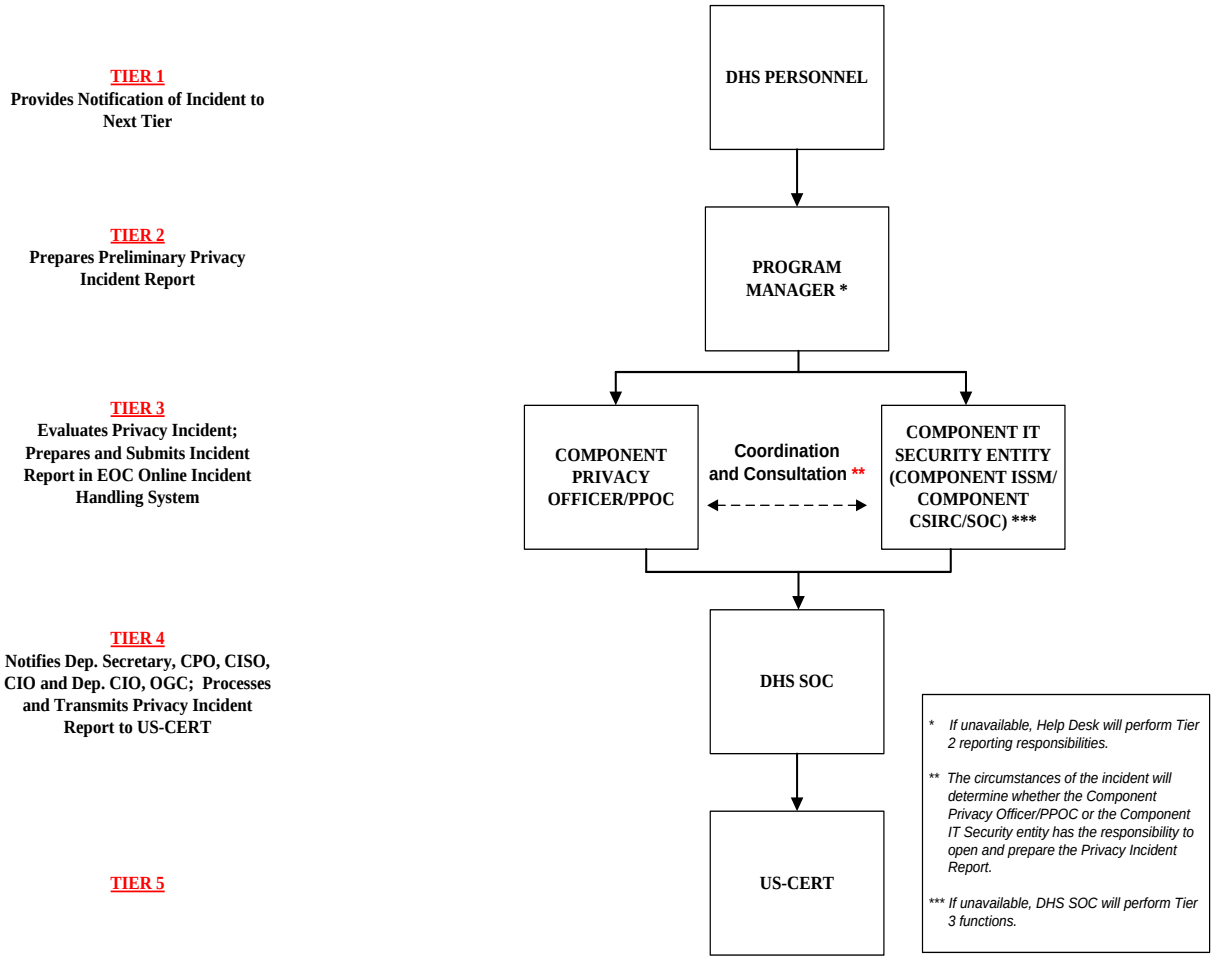

Diagram A: Reporting Process for Privacy Incidents

4.6. Supplementation of the Privacy Incident Report

After DHS SOC has reported the Privacy Incident to US-CERT, the Component Privacy Officer/PPOC must supplement the Privacy Incident Report, as appropriate, with any further factual information that will facilitate the handling of the Privacy Incident. Supplemental information can include factual information solicited by US-CERT, or other information related to the escalation, investigation, notification, mitigation, or incident closure stages of incident handling.

4.7. Internal Notification of DHS Senior Officials

4.7.1. Notification of the DHS Deputy Secretary, DHS CPO, DHS CIO, DHS Deputy CIO, DHS OGC, and DHS CISO

When DHS SOC transmits the Privacy Incident Report to US-CERT, DHS SOC simultaneously and automatically issues a Privacy Incident Notification to senior officials including, but not limited to, the Deputy Secretary, DHS CPO, DHS CIO, DHS OGC, DHS Deputy CIO, DHS CISO, and DHS Privacy Office, Director of Privacy Incidents and Inquiries, alerting them of the transmission of the Privacy Incident report to US-CERT. All Tier 2 and 3 personnel from the affected Component are included in the notification. See Diagram B for an illustration of the DHS organizational process for notifying DHS senior officials and appropriate authorities at DHS of a Privacy Incident.

4.7.2. Notification of the DHS Secretary, DHS CSO and DHS CFO

The circumstances under which the DHS Secretary, DHS CSO and DHS CFO will be notified of a Privacy Incident are set forth in Section 5.4.5 of this guidance.

4.8. Notification of External Entities

4.8.1. US-CERT Notifies and Coordinates with Appropriate Government Agencies

Within one hour of its receipt of a Privacy Incident Report, US-CERT will coordinate with and notify appropriate officials. See Diagram B for an illustration of the DHS organizational process for notifying senior DHS officials and for notifying appropriate authorities of a Privacy Incident at DHS.

4.8.2. DHS or Component CFO Notifies Affected Bank

If the Privacy Incident involves government-issued credit cards, the DHS or Component CFO will promptly notify the issuing bank of the Privacy Incident. See Diagram B for an illustration of the DHS organization structure for this notification process. The DHS or Component CFO must also notify the bank or other entity involved when the Privacy Incident involves individuals' bank account numbers used for direct deposit of credit card reimbursements, government salaries, travel vouchers, or any benefit payment.

The DHS or Component CFO will inform the Component Privacy Officer/PPOC of the affected Component when the notification occurs. The Component Privacy Officer/PPOC will supplement the Privacy Incident Report to reflect the notification of affected bank(s).

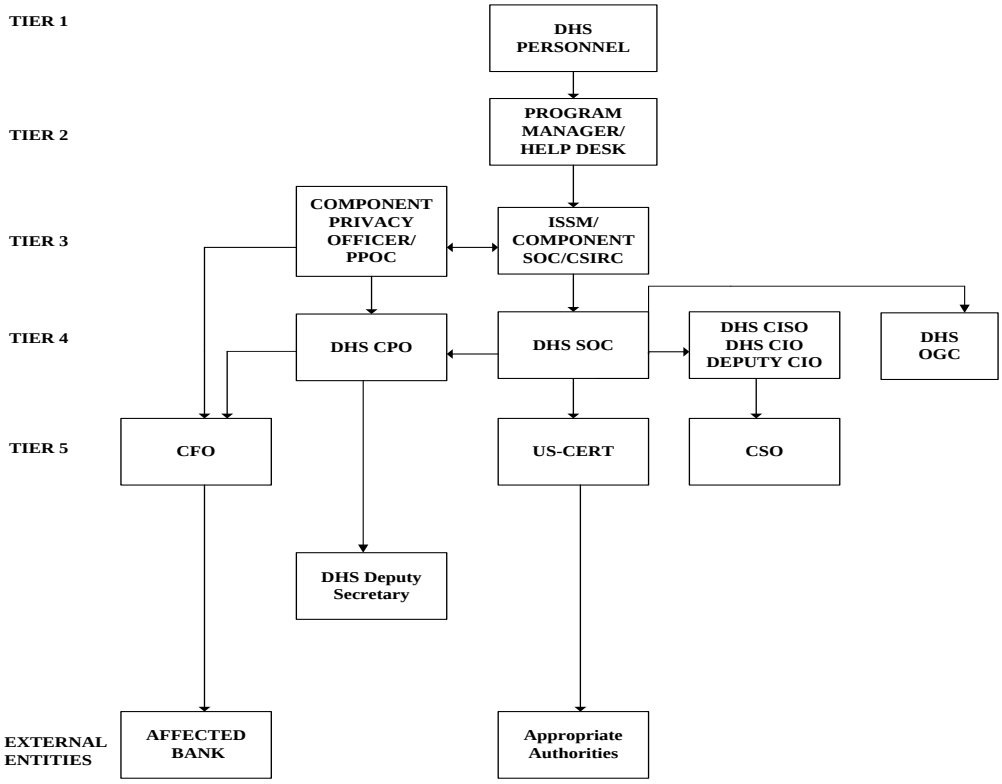

Diagram B: Organization Process for Notifying Senior DHS Officials and Notification of External Entities

5. Escalation

The escalation process involves a risk-based analysis that will enable DHS to tailor its response to a Privacy Incident based upon the severity of the incident. Using the PIHG, the Component Privacy Officer/PPOC will conduct a risk analysis of the incident, and will consult with the Component IT Security Entity if the incident impacts the security of a DHS IT system.

Once the Privacy Incident has been reported to DHS SOC, the Component Privacy Officer/PPOC must immediately evaluate the context of the incident and the PII that was potentially or actually lost or compromised in the incident. The Component Privacy Officer/PPOC must use their best judgment in using the following methodology:

1. Evaluate the five factors set forth in Section 5.3 to determine the likely risk of harm posed by the Privacy Incident;
2. Assign an impact level of low, moderate, or high to each risk factor;
3. Recommend who should handle the incident (e.g., Component Privacy Officer/PPOC, or specialized PIRT) for purposes of investigation, notification, mitigation, and closure;

4. Decide preliminarily whether notification is warranted; and
5. Identify the steps DHS should take to mitigate the risk of harm.

The Component Privacy Officer/PPOC may conduct the risk analysis using the Escalation Risk Assessment in the DHS EOC Online Incident Handling System. The Escalation Risk Assessment may be uploaded to the Privacy Incident Report in the DHS EOC Online Incident Handling System to supplement the report. *See Appendix E, Escalation Risk Assessment template,* and *Appendix D, DHS Privacy Playbook: Handling Process Overview,* for an overview of the escalation process.

The timing and sequence of events during escalation may vary from one incident to another. The requirements of incident handling necessitate prompt decision-making concerning the escalation. Therefore, the Component Privacy Officer/PPOC will be given a certain degree of flexibility and latitude. Escalation decisions that are verbal may be included in the DHS EOC Online Incident Handling System.

5.1. The Initial Risk Analysis – Five Risk Analysis Factors

In developing the appropriate DHS response to a Privacy Incident, the Component Privacy Officer/PPOC must first assess the likely risk of harm caused by the incident and then assess the level of risk. This is a *preliminary assessment based upon the facts known at that time*. Therefore the assessment may change as additional facts develop during incident handling.

The factors that help address the likely risk of harm posed by a Privacy Incident are:

- The nature of the data elements involved (Section 5.3.1)
- The number of individuals affected (Section 5.3.2)
- The likelihood that PII is accessible and usable (Section 5.3.3)
- The likelihood that a Privacy Incident may lead to harm (Section 5.3.4)
- The ability to mitigate the risk of harm (Section 5.3.5)

In analyzing a Privacy Incident, the first step the Component Privacy Officer/PPOC should take is to evaluate whether the data elements constitute the type of information that may pose a risk of identity theft. If identity theft is not implicated, the Component Privacy Officer/PPOC will proceed with the assessment of the five factors with assistance, as needed from the DHS Privacy Office. If there is a risk of identity theft, specialized attention may be warranted. The Component Privacy Officer/PPOC should refer to Appendix F for substantive and procedural guidance concerning the handling of such incidents.

An impact level of low, moderate, or high will be assigned to each factor. The results will indicate who should handle the Privacy Incident (e.g., Component Privacy Officer/PPOC, Specialized PIRT).

5.2. Standards for Categorization of Privacy Incident: Assessing the Likely Risk of Harm

The Component Privacy Officer/PPOC will categorize the risk level of each factor as low, moderate, or high as follows:

Level of Impact		
Low	The loss of confidentiality, integrity, or availability is expected to have a **limited adverse effect** on organizational operations, organization assets or individuals.	(i) cause degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Moderate	The loss of confidentiality, integrity, or availability is expected to have a **serious adverse effect** on organizational operations, organization assets or individuals.	(i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries
High	The loss of confidentiality, integrity, or availability is expected to have a **severe or catastrophic adverse effect** on organizational operations, organization assets or individuals	(i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

5.3. Risk Analysis of Five Factors

5.3.1. Factor One: Nature of the Data Elements Involved in the Privacy Incident

The nature of the data elements compromised is a *key factor* in assessing whether escalation within DHS should occur, and in determining when and how DHS should provide notification to

affected individuals. It is difficult to characterize data elements as creating a low, moderate, or high risk simply based on the type of PII because the sensitivity of the data is determined by its use with other factors. A name in one context may be less sensitive than in another context. 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. Therefore, the nature of the data elements depends upon the *sensitivity* of the information and the contextual environment.

DHS personnel must use a best judgment standard in assessing the sensitivity of PII in its context. For example, an office contact list contains PII (name, phone number, etc.). 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. Sensitive PII results in a reasonably high risk of harm to the individual due to the sensitivity of the specific data elements. 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.

Risk Levels for Nature of Data Elements -- Examples	
Low	Compromise of a database containing the full names, office mailing addresses, and job titles of subscribers to agency media alerts.
Moderate	Compromise of a database containing the full names, home mailing addresses, and job titles of persons who had failed to complete DHS-required training for this year.
High	Compromise of a database containing the full names, home mailing addresses, and SSNs of individuals receiving disaster relief benefits.

5.3.2. Factor Two: Number of Individuals Affected

Components may also choose to consider how many individuals are identified in the information (e.g., number of records). 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 and the cost to the component in addressing the incident. For this reason, components may choose to set a higher impact level for particularly large PII datasets than would otherwise be set. However, components should not set a lower impact level for a PII dataset simply because it contains a small number of records.

This factor may directly impact the decision as to who should handle the Privacy Incident for purposes of investigation, notification, and mitigation. The magnitude of the number of affected individuals may dictate the methods chosen for providing notification, but should *not* be *the determining factor* for whether a component should provide notification. See Section 8.2.8 in Notification for a discussion of the means of notification.

Where notification to a large number of affected individuals may be warranted, a specialized PIRT should be convened to assist with logistical and substantive issues presented by the Privacy Incident.

5.3.3. Factor Three: Likelihood the PII is Accessible and Usable

The likelihood that PII will be used by unauthorized individuals must also be assessed. An increased risk that the information will be used by unauthorized individuals should influence the impact level assigned to this factor and ultimately the decision to provide notification.

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

The Component Privacy Officer/PPOC will first need to assess whether the PII is at a low, moderate, or high risk of being compromised. This assessment should be guided by NIST security standards and guidance. Other considerations may include the likelihood that any unauthorized individual will know the value of the information and either use the information or sell it to others.

Likelihood the PII is Usable -- Examples	
Low	Email was sent that contained the names and the last four digits of government-issued credit card numbers of employees in the Component who have purchasing authority. The email containing PII was protected by a strong password, but was sent to an individual at another component who did not have a need to know the information.
Moderate	Laptop was lost that contained the names, government-issued credit card numbers, and Personal Identification Numbers (PIN) of employees in the Component who have purchasing authority. Although the database containing PII was encrypted, the encryption used was the 40-bit secure socket layer (SSL) standard which is not validated by NIST.
High	Laptop was stolen that contained the names, government-issued credit card numbers, and PINs of employees in the Component who have purchasing

	authority; laptop containing PII was not encrypted or password protected.

5.3.4. Factor Four: Likelihood that the Privacy Incident May Lead to Harm to the Individual or to the Agency

5.3.4.1. Broad Reach of Potential Harm

A broad reach of potential harm must be considered. The Privacy Act of 1974 requires federal agencies to protect against any anticipated threats or hazards to the security or integrity of records that could result in "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." (5 U.S.C. § 552a(e)(10)). 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 pain and emotional distress;
- The disclosure of address information for victims of abuse;
- The potential for secondary uses of the information which could result in fear or uncertainty; or
- The unwarranted exposure leading to humiliation or loss of self-esteem.

5.3.4.2. Likelihood Harm Will Occur

The likelihood an incident may result in harm depends on the manner of the actual or suspected loss or compromise of PII and the type(s) of PII involved in the incident.

Likelihood PII May Lead to Harm Examples	
Low	List containing the names, office addresses, and badge numbers of individuals who have completed DHS-required training.
Moderate	List containing the names, office addresses, and badge numbers of individuals who failed to complete DHS-required training.
High	List containing the names, components, and office addresses of individuals who are under Departmental investigation for misconduct.

If the Privacy Incident includes any of the following types of or combinations of Sensitive PII, the incident may pose a risk of harm to include identity theft:

- SSN

- Any government-issued identification number (e.g., driver's license or state identification number, passport number)
- Alien Registration Number
- Financial account number
- Biometric identifier (e.g., fingerprint, iris scan, voice print)
- A name, address, or telephone number, combined with:
  - Citizenship or immigration status;
  - Other data used by DHS to identify or authenticate an individual's identity, such as a fingerprint identification number (FIN) or Student and Exchange Visitor Information System (SEVIS) identification number;
  - Medical information; or
  - Date of birth, password, or mother's maiden name

All Sensitive PII must be categorized as MODERATE or HIGH.

For additional information regarding Identity Theft, refer to Appendix F.

See Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS at http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_spii_handbook.pdf.

5.3.5. Factor Five: Ability to Mitigate the Risk of Harm

The risk of harm will depend on the ability of DHS to mitigate further compromise of the PII affected by the incident. Appropriate countermeasures such as monitoring systems to identify patterns of suspicious behavior should be taken. For example, if the information relates to disaster relief beneficiaries, monitoring the beneficiary database for duplicate requests may signal fraudulent activity. Such mitigation may not prevent the use of the PII for identity theft, but it could limit the associated harm. Some harm may be more difficult to mitigate than others, particularly where the potential injury is more individualized and may be difficult to determine.

Ability to Mitigate the Risk of Harm Examples	
Low	A document containing the name, weight, height, eye and hair color of several new employees was mistakenly faxed from the Component's security office to a government agency that was not authorized to receive the information. The Component's security officer does not believe the information was compromised because the unauthorized recipient promptly destroyed the information as requested soon after it was received.
Moderate	An employee reports he had inadvertently acquired access to five other employees' government credit card numbers located on travel vouchers in the

	Component's Travel Management System. The Component CFO notifies the issuing banks of the incident and the accounts are immediately closed.
High	A document containing the background investigation summary reports for a dozen DHS employees is posted on the Component's intranet. Upon learning of the incident, the Component immediately removes the posting from the intranet and the server, and notifies the affected employees of the posting.

5.3.6. Balancing the Five Factors in Determining the Severity of Incident Based Upon the Likely Risk of Harm Posed by the Incident

After the five risk analysis factors have been evaluated, the Component Privacy Officer/PPOC will balance the impact levels of the factors to ascertain the severity of the incident. Given that the nature of the data elements involved in the Privacy Incident is a *key factor* in the risk analysis, the impact level assigned to this factor should be the starting point for assessing the overall severity of the incident. The decision to provide notification should give greater weight to Factor Three (i.e., the likelihood the information is accessible and usable) and Factor Four (i.e., whether the Privacy Incident may lead to harm).

Consider the following example and related risk analysis:

Balancing Risk Analysis Factors to Ascertain Severity of the Incident Example	
Example	Package containing two Alien Files was temporarily lost that contained the names, SSNs, Alien Registration Numbers, addresses, and dates of birth. The package was located shortly thereafter. The investigation revealed that the package was not opened and there was no access or distribution of information.
Analysis	The names, SSNs, Alien Registration Numbers, addresses, and dates of birth are data elements that are commonly used in identity theft and thus warrant an impact level of **high**. Also, identity theft is a substantial harm that could result from the compromise of this information; therefore, Factor Four would be categorized as **high** as well. The PII was sent by certified mail and sealed in accordance with the Component's mailing policies. There was no evidence that the information was accessed or distributed. Therefore, Factor Three (i.e., the likelihood that the PII is accessible and useable) would have an impact level of **low**. Additionally, the package was promptly located and inspected to ensure that the information was neither accessed nor distributed. Therefore, Factor Five (i.e., the ability to mitigate the risk of harm) would have an impact level of **low**. Although the factors related to the nature of the PII and likelihood the PII may lead

	to harm may have high impact levels, the overall severity of the incident is **adjusted downward** because of the low impact levels assigned to Factor Three (i.e., likelihood of compromise) and Factor Five (i.e., mitigation). Therefore, the **severity of the incident would be low**.

5.4. Determining Who Will Handle the Privacy Incident

The Component Privacy Officer/PPOC will determine who handles the remaining stages of the Privacy Incident based on the severity of the incident. This section describes who may handle a Low-, Moderate-, or High-Impact Privacy Incident and also identifies the DHS senior officials who must be notified of the incident. Diagram C displays the decision-making process for this section.

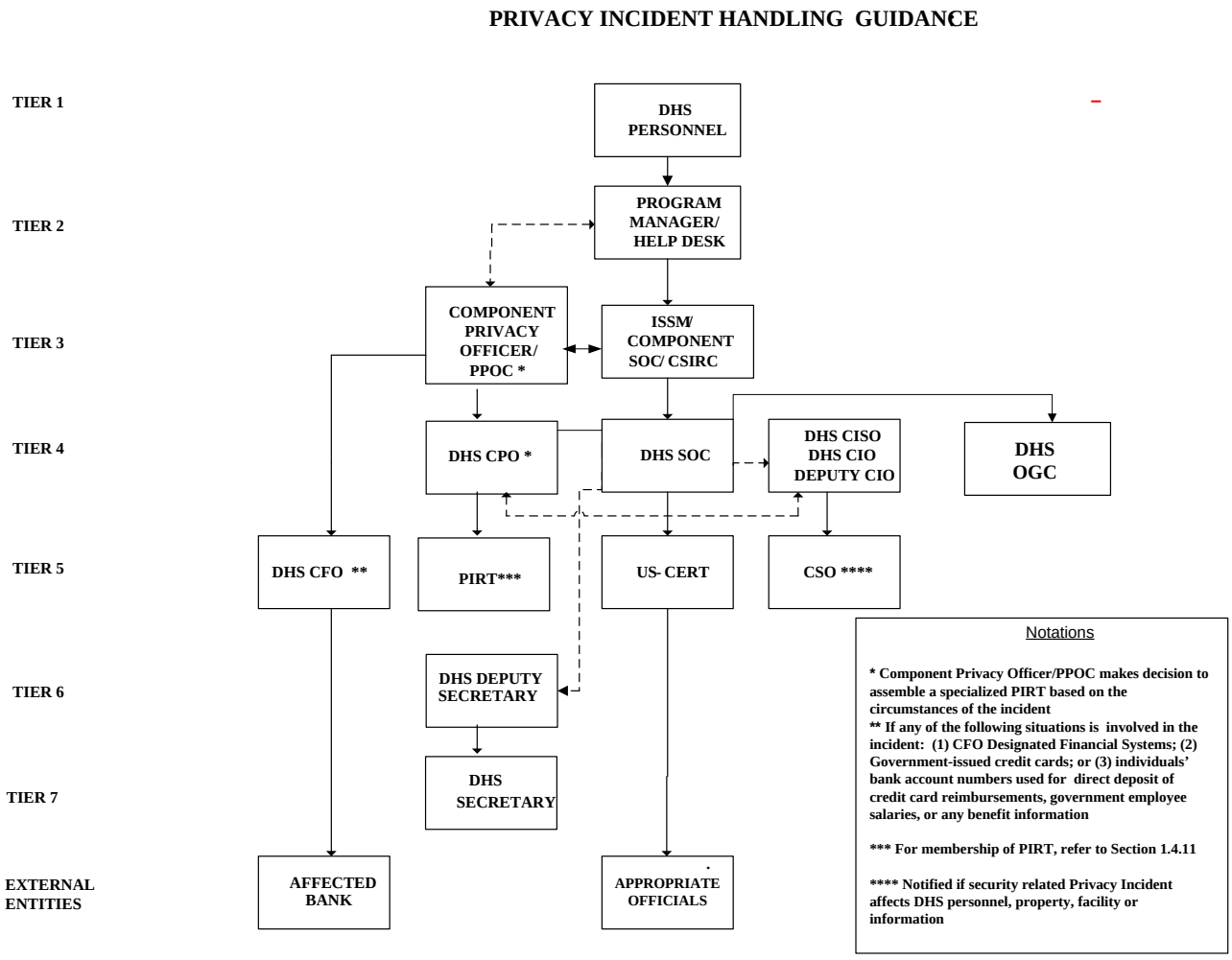

Diagram C: Process Flow for Escalation of Privacy Incident

5.4.1. Privacy Incidents with a Low Potential Impact

Privacy Incidents with a LOW potential impact do not create a reasonable risk of harm and can be handled with minimum resources by the Component Privacy Officer/PPOC. DHS has determined that certain low risks must be accepted in order to ensure that resources are available to address more serious incidents. Not all incidents necessitate the significant allocation of DHS resources for handling such as Low-Impact incidents. Therefore, the Component Privacy Officer/PPOC will be responsible for handling Low-Impact Privacy Incidents, with guidance, as needed, from the DHS Privacy Office.

5.4.2. Privacy Incidents with a Moderate or High Potential Impact

If the incident meets or exceeds the reasonable risk of harm standard, its potential impact will be Moderate or High. The likely risk of harm for an incident in which criminal activity is suspected or confirmed is MODERATE or HIGH. Incidents involving Sensitive PII are always designated as MODERATE or HIGH impact.

The Component Privacy Officer/PPOC will use his or her best judgment in determining who would comprise the PIRT to handle a Moderate-Impact incident occurring at the Component level. A specialized PIRT may be convened when the *potential impact* of the Privacy Incident occurring at the Component level is MODERATE according to Section 5.2. See Section 1.4.11 when considering enhancing the PIRT. A specialized PIRT may be convened when the *potential impact* of the Privacy Incident is HIGH according to Section 5.2, or when the *potential impact* of the incident is MODERATE but occurred at DHS Headquarters. The PIRT members will provide advice and assistance as needed to address the incident.

5.4.3. Special Circumstances Warranting Escalation to the DHS CFO or Component CFO

The Component Privacy Officer/PPOC will notify the DHS or Component CFO of any Privacy Incident involving government-issued credit cards or individuals' bank account numbers used for direct deposit of credit card reimbursements, government employee salaries, or any benefit information. The DHS or Component CFO will notify the affected bank(s) and CHCO of the incident when appropriate. The Component Privacy Officer/PPOC will supplement the Privacy Incident Report to reflect the CFO's notification of the affected bank(s) and ensure the DHS or Component CFO is a part of a specialized PIRT as necessary.

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.

5.4.4. Special Circumstances Warranting Escalation to the DHS CSO

The DHS CIO will notify the DHS CSO when the Privacy Incident involves security-related issues affecting DHS personnel, property, facilities, and information. Escalation steps taken must be documented in the Privacy Incident Report.

5.4.5. Escalation to and Notification of the DHS Deputy Secretary and the DHS Secretary

The DHS SOC will notify the DHS Deputy Secretary of a Privacy Incident simultaneously with or immediately following the transmission of a Privacy Incident Report to US-CERT. The DHS Deputy Secretary will use his/her best judgment in determining whether the DHS Secretary should be notified of a Privacy Incident.

5.4.6. Preliminary Recommendation Regarding External Notification of Affected Individuals

In the Privacy Incident Report, the Component Privacy Officer/PPOC will make a preliminary recommendation of whether external notification is warranted. Privacy Incidents are fact-specific and context-dependant and notification is not always necessary or desired. Notification should only be given in those instances when there is a reasonable risk of harm and the decision will not lead to the overuse of notification.

To determine whether notification of an incident is required, the component should first assess the likely risk of harm caused by the incident, and then assess the level of risk. Components should consider a wide range of harms, such as harm to reputation and the potential for harassment or prejudice, particularly when health or financial benefits information is involved in the incident. Notification of those affected and/or the public allows affected individuals the opportunity to take steps to help protect themselves from the consequences of the Privacy Incident. Therefore, an increased risk that the PII will be used by unauthorized individuals should influence the decision to provide notification. Other considerations may include the likelihood that any unauthorized individual will know the value of the information and either use the information or sell it to others.

Under circumstances when notification could increase a risk of harm, the wise course of action may be to delay notification. Additionally, it is important that notification be consistent with the needs of law enforcement and national security, as well as any measures necessary for DHS to determine the scope of the incident and, if applicable, restore the reasonable integrity of the data system. See Section 8 for the procedure for external notification; Section 8.2 sets forth the timing, method, and means of notification.

The Component Privacy Officer/PPOC should give careful consideration in deciding whether notification is warranted. When there is little or no risk of harm, notification might create unnecessary concern and confusion. The cost to individuals of responding to notices when the risk of harm may be low should be considered. Moreover, sending too many notices based on

overly strict criteria could render all such notices less effective because affected individuals could become desensitized and fail to act even when risks are truly significant.

6. Mitigation

6.1. Purpose of Mitigation: Containment of Source and Prevention or Minimization of Consequential Harm

DHS must be able to respond quickly and effectively to mitigate the adverse effects of a Privacy Incident. While assessing the level of risk in a particular incident, the Component should also consider options for reducing that risk. The Component Privacy Officer/PPOC, PIRT, Component IT Security Entity, and PM have a central role in implementing countermeasures to lessen the potential harm posed by the Privacy Incident. *See Appendix D, DHS Privacy Playbook: Handling Process Overview,* for an overview and checklist for the incident mitigation process. Mitigation is an essential aspect of the component's effort to contain the cause of the Privacy Incident, and identify and lessen the potential harm that the loss, compromise, or misuse of the PII may have on affected individuals.

6.2. Identification of Steps DHS Can Take to Mitigate the Harm

In the Privacy Incident Report, the Component Privacy Officer/PPOC and/or Component ISSM details whether and to what extent DHS may take countermeasures to mitigate the harm posed by the incident. Such steps may include eliminating unauthorized access to the PII, contacting the DHS OIG and law enforcement, notifying affected banks, and monitoring accounts for unauthorized use.

6.3. Timing and Sequence of Mitigation

Mitigation is not necessarily a linear process, but rather may occur concurrently with other processes (e.g., reporting, escalation, investigation, etc.), or repeatedly during the process of Privacy Incident handling. Mitigation measures should be implemented at varying times during the incident handling process as necessary.

6.4. Harm Defined

Harm is defined as:

> 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.

There is a wide range of harms that may be caused by a Privacy Incident, including anticipated threats or hazards to the security or integrity of records that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom information is maintained. The range of harm includes:

- Harm to reputation and the potential for harassment or prejudice, particularly when health or financial benefits information is involved;
- the effect of a breach of confidentiality or fiduciary responsibility;
- the potential for blackmail;
- the disclosure of private facts, mental pain, and emotional distress;
- the disclosure of address information for victims of abuse; and
- the potential for secondary uses of the information, which could result in fear or uncertainty; or the unwarranted exposure leading to humiliation or loss of self-esteem.

6.5. Division of Mitigation Responsibilities

The Component Privacy Officer/PPOC will work with the Component IT Security Entity, PIRT if convened, and PM to prevent or minimize any resulting harm. The first step of the mitigation process may be performed by the PMs by gathering, securing, and documenting evidence about the incident. Therefore, PMs will collaborate with the Component Privacy Officer/PPOC and the Component IT Security Entity regarding the identification of the source of the incident, and the implementation of measures to contain the initial harm resulting from the Privacy Incident.

The Component IT Security Entity will address IT security issues pertaining to the incident, and will implement containment measures for IT systems in accordance with the CONOPS and DHS 4300A Sensitive Systems Handbook. Responsibilities include:

- Containing the incident.
- Eliminating the incident.
- Identifying and mitigating all vulnerabilities that were exploited.
- Returning affected systems to an operationally ready state.
- Implementing additional monitoring to look for future related activity.

One goal of mitigation is to restore the integrity of the system, whether electronic or paper. Integrity for an electronic system includes the restoration of an affected system to an operationally ready state where the system is functioning normally. Integrity for a paper-based system includes the restoration of security measures protecting the paper information (e.g., replacement of locks, ensuring that all files are accounted for, etc.).

The Component Privacy Officer/PPOC will address the privacy ramifications of a Privacy Incident and focus on preventing or minimizing any subsequent harm to affected individuals. As such, mitigation will involve activity beyond the securing of the system (electronic or paper) and isolating the vulnerability. The Component Privacy Officer/PPOC should consider a broad range of defenses as determined by the nature and sensitivity of the PII. An effective response may call for 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 assisting in notification to affected

individuals or playing a role in preventing or minimizing harms from the incident. Mitigation may include:

- Notification to affected individuals, the public, and other government entities (e.g. Congress) pursuant to the procedures in Section 8 of this guidance.
- Removing information from an Internet or intranet page.
- Component Privacy Officer/PPOC in coordination with Component SOC or DHS SOC Government Watch Officer will ensure external notification to law enforcement for incidents that do not impact physical security. Such notification should be handled in consultation with the DHS CPO. If criminal activity impacting physical security is suspected, the Component Privacy Officer/PPOC in coordination with Component SOC or DHS SOC Government Watch Officer will ensure consultation and reporting with the Component CSO. Component CSO will determine whether contacting internal or external law enforcement is necessary.
- Notification and involvement of external law enforcement must be documented in the Privacy Incident Report.
- Contacting banks for incidents involving credit cards or bank accounts pursuant to Sections 4 and 5.
- Offering credit monitoring services or providing information on such services to mitigate the misuse of the PII and identify patterns of suspicious behavior.

6.6. Mitigation: Reducing the Risk after Disclosure

While assessing the level of risk in a given situation, the component should also consider options for reducing that risk. Certain options are available to components to help potential victims:

6.6.1. Mitigation: Protective Measures that DHS HQ Offices and Components Can Take

For Privacy Incidents where the compromised information presents a risk of new accounts being opened, components can consider protective measures, but they may involve additional expense. First, technology can help analyze whether a particular incident appears to result in identity theft. This analysis may be a useful intermediate protective action, especially when the component is uncertain about whether the identity theft risk warrants implementing more costly steps such as credit monitoring, or when the risk is such that components may want to do more than rely on the individual's action(s).

Second, components may provide credit monitoring services. Credit monitoring is a commercial service that can assist individuals in early detection of instances of identity theft. Although credit monitoring cannot guarantee that identity theft will not occur, it allows individuals to take steps to minimize the harm. A credit monitoring service notifies individuals of changes that appear in their credit report, such as creation of new accounts, changes to their existing accounts or personal information, or new inquiries for credit.

When deciding whether to offer credit monitoring services, including the type and length of service, components should consider the seriousness of the risk of identity theft arising from the Privacy Incident. Particularly important is whether use of the information has already been detected, and the cost of providing the service.

Finally, notification to law enforcement is an important way for a component to mitigate the risks faced by the potentially affected individuals. External notification to law enforcement when criminal activity is suspected or confirmed should be handled by Component CSO and/or DHS CSO depending on the level and severity of criminal activity. The Component Privacy Officer/PPOC will coordinate with Component SOC or DHS SOC Government Watch Officer. Notification and involvement of external law enforcement must be documented in the Privacy Incident Report. Because a Privacy Incident may be related to other incidents or other criminal activity, the DHS OIG and other DHS senior officials should coordinate with appropriate law enforcement to look for potential links, and to effectively investigate criminal activity that may result from, or be connected to, the Privacy Incident. See Section 7 for the investigation procedure.

6.7. Providing Notice to Those Affected

The notification procedures set forth in Section 8 of this guidance govern the decision to provide external notification.

6.8. Mitigation Countermeasures Must be Documented

All mitigation measures implemented must be documented in the Privacy Incident Report in the DHS EOC Online Incident Handling System.

7. Incident Investigation

All Privacy Incidents reported to US-CERT will be investigated to the extent warranted by the facts of the incident. *See Appendix D, DHS Privacy Playbook: Handling Process Overview*, for an overview and checklist for the investigation process. The Component Privacy Officer/PPOC or Component IT Security Entity will coordinate the following investigation procedures unless or until a lead investigator is designated:

- Limit internal notifications and access to those who have a legitimate need to know.
- Review what has occurred:
  - Gather and document all information necessary to describe and respond to the incident.
  - Review the Privacy Incident Report submitted to US-CERT and identify what additional information is necessary.
  - Confirm what personal information is lost or at risk.
  - Identify what steps have been taken to reduce the risk of harm.
- Develop a plan of action:

- If a specialized PIRT is convened, clearly define the responsibilities of each PIRT member based upon the capability, expertise, and authority of the member in order to ensure proper handling of the Privacy Incident and to avoid duplicative efforts.
- Identify the lead investigator for a particular Privacy Incident. It should be someone who is trained or familiar with incident response procedures, and the complexities involved with the potential loss or compromise of PII.
  - If no specialized PIRT is convened, the lead investigator will report to the Component Privacy Officer/PPOC or Component IT Security Entity. If the incident involves physical security, the lead investigator may report to the Component CSO. If a Moderate-Impact or High-Impact Privacy Incident is involved, the lead investigator may also report to the DHS OIG and DHS OGC.
  - The lead investigator should consult with Component OCC or DHS OGC before initiating an investigation into issues involving the handling of evidence and chain of custody.
- Follow the DHS internal incident handling procedures:
  - Identify what further steps must be taken to formulate any further response by DHS.
  - Identify information resources that have been affected and identify additional resources that might be affected.
  - Estimate the current and potential technical impact (e.g., data, database, system, or network) of the incident.
  - Back up the system in accordance with the standards and procedures set forth in DHS 4300A Sensitive Systems Handbook.

- Adhere to standard investigation procedures:
  - Create and maintain a complete record of the investigation.
  - Protect and preserve all evidence.
    - Consult with Component OCC or DHS OGC to address issues involving the handling of evidence and chain of custody.
    - Take precautions to prevent destruction or corruption of evidence that may be needed to support criminal prosecution.
    - Identify and properly secure all evidence to maintain its validity in court.
  - Create and maintain a chain of custody log of everyone who has access to the evidence. Keep a record of the individuals who have touched each piece of evidence. The record should include the date, time, and locations of where the evidence is stored.
  - Component Privacy Officer/PPOC, in coordination with Component SOC or DHS SOC Government Watch Officer, will ensure external notification of law enforcement for incidents that do not impact physical security. If criminal activity impacting physical security is suspected, the Component Privacy Officer/PPOC, in coordination with Component SOC or DHS SOC Government Watch Officer, will ensure

consultation and reporting with the Component CSO. Component CSO determines whether contacting internal or external law enforcement is necessary.

  - Notification and involvement of internal or external law enforcement must be documented in the Privacy Incident Report.
  - Protect the chain of custody of the backup data. Store the data in a secure location.

- Law enforcement will consult with the lead investigator and other PIRT members as warranted. For incidents where criminal activity is suspected or confirmed, the lead investigator will consult with law enforcement, DHS OIG, and the Component CSO regarding the closure of the investigation.
- Review events and actions at the conclusion of the incident and make recommendations to the DHS CPO, DHS CIO, and PIRT members regarding any suggested changes in the DHS technology and incident handling plan.
- Advise the DHS Deputy Secretary, DHS CPO, DHS CIO, DHS Deputy CIO, DHS OIG, and DHS CISO about the investigation as circumstances warrant. The DHS CPO will consult with DHS senior officials as needed.

  Upon completion of the investigation, the Component Privacy Officer/PPOC will update the Privacy Incident Report at https://eoconline.dhs.gov to indicate closure of the investigation, subject to review by the DHS CPO and DHS CIO.

8. Notifications and Communications Concerning Privacy Incidents

An effective and meaningful response to the incident requires prompt notification to DHS senior officials at various stages of the Privacy Incident handling process. DHS components, employees, and officials must follow the procedures set forth in Section 8.1 governing internal notification to DHS senior officials and in Section 8.2 governing the authorization of external notification. *See Appendix D, DHS Privacy Playbook: Handling Process Overview,* for an overview and checklist for the incident notification process.

8.1. Internal DHS Notification Procedures

Internal notifications may take two forms: (1) Privacy Incident Notifications automatically generated by the DHS EOC Online Incident Handling System; or (2) Notifications sent by email or voicemail. Internal notifications and access must be limited to those who have a legitimate need to know.

8.1.1. Privacy Incident Notifications Automatically Sent to Officials by the DHS EOC Online Incident Handling System

When DHS SOC transmits the Privacy Incident Report to US-CERT, DHS SOC simultaneously and automatically issues a Privacy Incident Notification to senior officials including, but not limited to, the Deputy Secretary, DHS CPO, DHS CIO, DHS OGC, DHS Deputy CIO, DHS

CISO, and DHS Privacy Office, Director of Privacy Incidents and Inquiries, alerting them of the transmission of the Privacy Incident report to US-CERT. All Tier 2 and 3 personnel from the affected Component are included in the notification. See Section 4.5 for additional information regarding the Tiers.

8.1.2. Internal Notification by Email and/or Phone Call

Notification must be provided under the following circumstances:

- After DHS SOC reports the Privacy Incident to US-CERT, a specialized PIRT may be convened for incident handling. The Component Privacy Officer/PPOC will notify members of this PIRT by email or phone that a Privacy Incident has been reported to US-CERT, and that they are responsible for handling the investigation, notification, and mitigation for the Privacy Incident.
- When DHS SOC has reported an incident solely as a Computer Security Incident and then subsequently determines that the incident involved the potential compromise of PII, DHS SOC will notify the DHS Deputy Secretary, DHS CPO, DHS CIO, DHS Deputy CIO, DHS CISO, and DHS OGC of the change in categorization of the incident.
- If it is determined that additional Components are affected by the Privacy Incident, the Component Privacy Officer/PPOC must notify those components directly and document notification in the Privacy Incident Report.

8.2. External Notification Procedures

8.2.1. Disclosure of Privacy Incident Information by DHS Personnel Prohibited

Unless authorized pursuant to this guidance, DHS personnel should not disclose or cause to be disclosed any information pertaining to an ongoing or closed Privacy Incident to any person who does not have an authorized need to know the information.

8.2.2. Public Inquiries About Privacy Incidents

With respect to all media-related inquiries about Privacy Incidents, the DHS Public Affairs Office or the Component's Public Affair Office will be the point of contact.

For all non-media-related inquiries concerning the status of Privacy Incidents or the implementation of this guidance, the DHS CPO or DHS Privacy Office, Director of Privacy Incidents and Inquiries, will determine who will handle the inquiry.

8.2.3. Internal Decision-Making Process for External Notification

Once the Component Privacy Officer/PPOC has completed the Privacy Incident Report, a decision to publicly release information may be reached through collaboration with the Component Head and specialized PIRT if convened. If notification is warranted, the Component

Privacy Officer/PPOC, and specialized PIRT members, will assess the following issues concerning how and when notification outside DHS should be given:

- Timeliness of the Notification (Section 8.2.5)
- Source of the Notification (Section 8.2.6)
- Contents of the Notification (Section 8.2.7)
- Means of Providing the Notification (Section 8.2.8)
- Who Receives Notification: Public Outreach in Response to a Privacy Incident (Section 8.2.9)

On occasion, the DHS CPO or DHS Privacy Office, Director of Privacy Incidents and Inquiries, may need to coordinate with the DHS Public Affairs Office to provide *reasonable advance internal notice* to DHS senior officials by email or voicemail of a notification decision before external notification is made.

8.2.4. Authorization Required for External Communications

Authorization is required for external communications. This restriction is subject to Section 8.2.1 and applies to all external communications, including congressional notifications, press releases, and notifications to individuals potentially affected by the Privacy Incident.

8.2.5. Timeliness of the Notification

Before external 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 persons should be notified without unreasonable delay following the discovery of a 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.

Decisions to delay notification should be made by the DHS Secretary or a senior-level official that he/she designates in writing. In some circumstances, law enforcement or national security considerations may require a delay in notification if it seriously impedes the investigation of the Privacy Incident.

8.2.6. Source of Notification

As a general rule, notification to individuals affected by the Privacy Incident will be issued by the Component Head or the Component Privacy Officer/PPOC if appropriate. If warranted by the circumstances, the DHS CPO or the DHS Privacy Office, Director of Privacy Incidents and Inquiries, will issues the notification.

When the Privacy Incident involves a federal contractor or a public-private partnership operating a system of records on behalf of the component, DHS is responsible for ensuring that any notification and corrective action is taken. 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.

8.2.7. Contents of the Notification

8.2.7.1. General Requirements

The notification should be provided in writing and be in concise, plain language. The notice should include the following elements:

- 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, etc.)
- 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 individuals can take to protect themselves from potential harm
- What the component is doing to investigate the Privacy Incident, mitigate losses, and protect against a likely recurrence
- Who affected individuals should contact at the component for more information, including a telephone number, email address, and postal address.

A copy of a sample notification letter is attached to this guidance in Appendix G.

8.2.7.2. Translation of Notice into Other Languages

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).

8.2.8. Means of Providing Notification

The best means for providing notification will depend on the number of individuals affected and the contact information available about the affected individuals. The means selected by the Component to notify affected individuals must be based on the number of persons affected by

the Privacy Incident, and the urgency with which they need to receive notice. The following examples are types of notice which may be considered.

8.2.8.1. Telephone

Telephone notification may be appropriate in those cases where 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.

8.2.8.2. First-Class Mail

First-class mail should be the primary means of notification, and should be sent independent of other correspondence to the individual's last known mailing address in DHS records. When there is reason to believe the address is no longer current, reasonable steps must be taken to update the address by consulting with other agencies such as the U.S. Postal Service. The front of the envelope should be labeled with the name of your component as the sender to reduce the likelihood that the recipient thinks it is advertising mail.

8.2.8.3. Email

Notification to DHS employees via their government email addresses can also be considered as a primary means of notification. Email notification to individuals' personal email addresses can be problematic because they change their email addresses and often do not notify third parties of the change. However, when an individual has provided an email address to DHS, and has expressly given consent to email as the primary means of communication with DHS or with the affected component, and no known mailing address is available, notification by email may be appropriate. Email notification may include links to the component and www.USA.gov web sites, where the notice may be "layered" so the most important summary facts are provided first with additional information provided under link headings.

8.2.8.4. Existing Government Wide Services

The affected Component(s) should use government-wide services already in place to provide support services needed, such as USA Services including toll free number of 1-800-FedInfo and www.USA.gov.

8.2.8.5. Newspapers or other Public Media Outlets

Additionally, individual notification may be supplemented by placing notifications in newspapers or other public media outlets. The affected Component may set up toll-free call centers staffed by trained personnel to handle inquiries from the affected individuals and the public. *See Appendix H for a Sample Press Release.*

8.2.8.6. Substitute Notice

Substitute notice may be appropriate in instances where DHS does not have sufficient contact information to provide notification. Substitute notice should include a prominent posting of the notice on the DHS home page or the affected Component's website. Substitute notification can also be made to major print and broadcast media, including major media in areas where the affected individuals reside. The notice to media should include a telephone number where an individual can learn whether or not his/her personal information is included in the Privacy Incident.

8.2.8.7. Accommodations

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 website.

8.2.9. Who Receives Notification: Public Outreach in Response to a Privacy Incident

8.2.9.1. Notification of Individuals

The final consideration in the notification process is to whom the affected Component(s) should provide notification – the affected individuals, the public 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. *See Appendix G for a copy of a sample notification letter.*

8.2.9.2. Notification of Third Parties including the Media

DHS and its Components should consider the following guidelines when communicating with third parties regarding a Privacy Incident.

8.2.9.2.1. Careful Planning

The decision to notify the public media requires careful planning and execution so as not to unnecessarily alarm the public. When appropriate, public 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. Notification may be delayed at the request of law enforcement or national security agencies as described above in Section 8.2.5. 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 or the Component's Office of Public Affairs. *See Appendix H for a copy of a sample press release.*

8.2.9.2.2. Web Posting

DHS can post information about the Privacy Incident and notification in a prominent location on the home pages of DHS or the Component's 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 Frequently Asked Questions (FAQs) and other talking points to ensure the public understands the Privacy Incident and the notification process. The information may also appear on the www.USA.gov website. The affected Component may also consult with General Services Administration (GSA) USA Services to use their call center.

8.2.9.2.3. Notification of other Public and Private Sector Agencies

The Component Head and Component Privacy Officer/PPOC for the affected Component will work in consultation with the DHS CPO and DHS CIO to determine whether other public and private sector agencies may need to 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 stemming from the Privacy Incident. For example, a Privacy Incident involving medical information may warrant notification of the Privacy Incident to health care providers and insurers through the public or specialized health media; and a Privacy Incident of financial information may warrant notification to financial institutions through the federal banking agencies. 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.

8.2.9.2.4. Congressional Inquiries

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 CPO, DHS CIO and DHS Legislative Affairs Office will work closely to determine when notification of the incident should be provided to congressional oversight committee chairs. With respect to a High-Impact Privacy Incident, DHS Legislative Affairs Office and DHS Public Affairs Office 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.

8.2.9.3. Reassess the Level of Impact Assigned to the Information

After evaluating each of these factors, the previous levels of impact assigned to the information under NIST standards must be reviewed and reassessed. The impact levels – low, moderate, and high - describe the potential impact of the incident on the component or affected individual. The determination of potential impact of loss of information is made by DHS during an information system's C&A process. See FIPS Pub 199, February 2004; http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

- **Low** is defined as the loss of confidentiality, integrity, or availability, which could have a **limited** adverse effect on organizational operations, organizational assets or individuals

- **Moderate** is defined as the loss of confidentiality, integrity, or availability, which could have a **serious** adverse effect on organizational operations, organizational assets, or individuals.
- **High** is defined as the loss of confidentiality, integrity, or availability, which could have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

The impact levels will help determine when and how notification should be provided. Where there is a range of risk levels attributed to the factors, the decision to provide notification should give greater weight to the likelihood that the information is accessible and usable, and whether the Privacy Incident may lead to harm. If agencies appropriately apply the five risk factors discussed in Section 5.3 within the fact-specific context, it is likely that notification will only be given when there is a reasonable risk of harm and when it will not lead to the overuse of notification.

8.3. Documentation of External Notification in DHS EOC Online Incident Handling System

Documents pertaining to the internal decision-making process (e.g., External Notification Assessment, press release, notification letter to affected individual(s)) can be attached to the Privacy Incident Report in the DHS EOC Online Incident Handling System.

9. Consequences and Accountability for Violation of Federal Laws, Regulations, or Directives or DHS Policy

9.1. Overview

DHS personnel, including employees, supervisors, managers, and contractors, have privacy and security responsibilities to safeguard PII in accordance with federal laws, regulations, and directives, and Departmental directives and guidance. *See listing of authorities in Section 1.3.*

9.2. Privacy and Data Security Policies

Numerous regulations place restrictions on the government's collection, use, maintenance, and release of information about individuals. Regulations also place requirements on agencies to protect PII, which is defined as information in a system or online collection that directly or indirectly identifies an individual. For a comprehensive definition of PII, refer to Section 1.4.9.

9.3. Basis for Disciplinary or Corrective Action

Individuals who fail to implement such safeguards will face the consequences and will be held accountable through disciplinary or corrective action. The definitions of disciplinary and

corrective action are set forth in the *Standards of Ethical Conduct for Employees of the Executive Branch* and are:

- *Disciplinary Action* includes those disciplinary actions referred to in Office of Personnel Management (OPM) regulations and instructions implementing provisions of title 5 of the United States Code or provided for in comparable provisions applicable to employees not subject to title 5, including but not limited to reprimand, suspension, demotion, and removal. In the case of a military officer, comparable provisions may include those in the Uniform Code of Military Justice.
- *Corrective Action* includes any action necessary to remedy a past violation or prevent a continuing violation, including but not limited to restitution, change of assignment, disqualification, termination of an activity, waiver, or counseling.

Standards of Ethical Conduct for Employees of the Executive Branch, 5 C.F.R. §§ 2635.102(e) and (g); **http://www.usoge.gov**; see also *Ethics/Standards of Conduct*, DHS MD 0480.1 (March 1, 2003).

Disciplinary or corrective action regarding DHS personnel (i.e., employees, supervisors, and managers) may be based on the following:

- Failure to implement and maintain security controls, for which an employee is responsible and aware, for PII regardless of whether such action results in the loss of control or unauthorized disclosure of PII;
- Exceeding authorized access to, or intentional disclosure to unauthorized persons of, PII;
- Failure to report any known or suspected loss of control or unauthorized disclosure of PII;
- For managers and supervisors, failure to adequately instruct, train, or supervise employees in their responsibilities; and
- For managers and supervisors, failure to take appropriate action pursuant to PII handling requirements upon discovering a Privacy Incident or failure to implement and maintain required security controls and to prevent a Privacy Incident from occurring.

9.4. Consequences

Applicable consequences may include reprimand, suspension, removal, or other actions in accordance with applicable law and agency policy. At a minimum, DHS will remove the authority to access information or systems from any individual who demonstrates egregious disregard or a pattern of error in safeguarding PII.

DHS Policy
a. IT security-related and privacy-related violations are addressed in the *Standards of Ethical Conduct for Employees of the Executive Branch,* 5 CFR § 2635, and DHS employees may be subject to disciplinary action for failure to comply with DHS security and privacy policy, whether or not the failure results in criminal prosecution.
b. Non-DHS federal employees or contractors who fail to comply with Department security and privacy policies are subject to termination of their access to DHS IT systems and facilities, whether or not the failure results in criminal prosecution.
c. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions.

9.5. Procedure

The Component Privacy Officer/PPOC may inform the head of the Component, DHS OGC, and Component OCC, when DHS personnel have failed to implement safeguards to protect PII, or when a Privacy Incident arose from a violation or potential violation by DHS personnel of applicable laws, regulations, policies or directives governing the protection of PII. The DHS OGC or Component OCC will consult with the Component Privacy Officer/PPOC, Component Head, and CHCO on legal issues pertaining to disciplinary or corrective action.

Component Heads are responsible for taking corrective and disciplinary actions when security or Privacy Incidents and violations occur, and for holding personnel accountable for intentional transgressions. Consequences should be equal to the level of responsibility and type of PII involved. As with any disciplinary or corrective action, the particular facts and circumstances, including whether the incident was intentional, will be considered in taking appropriate action. Any action taken must be consistent with law, regulation, applicable case law, and any relevant collective bargaining agreement. The head of the Component will work with the Designated Agency Ethics Officials, as well as DHS OIG, DHS OGC and CHCO, in the event that the Privacy Incident arises from violations or potential violations of the ethics statutes or regulations. *See DHS 4300A Sensitive Systems Handbook; see also Appendix D, DHS Privacy Playbook: Handling Process Overview, for an overview and checklist for the process for pursuing disciplinary or corrective action.*

9.6. Privacy Incident Report May Include Description of the Violations of Law, Regulation, or Policy and Explanation of Corrective or Disciplinary Action Taken

The Component Privacy Officer/PPOC may document in the Privacy Incident Report any violation(s) or potential violation(s) that caused or contributed to, in part or whole, the Privacy Incident without naming personnel. No specific PII may be disclosed in the Privacy Incident Report. The Privacy Incident Report can contain, if known, an explanation of the following:

- Violation(s) of federal laws or regulations, DHS policy set forth in this guidance or DHS 4300A Sensitive Systems Handbook, or DHS management directives.

- Corrective or disciplinary action(s) taken; if no action is taken, then a statement to that effect is required.
- If the Privacy Incident involves potential criminal activity and has been turned over to internal or external law enforcement, this fact should be reported.

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 CHCO must maintain a record of all disciplinary or corrective actions taken against DHS personnel that arise out of a Privacy Incident.

10. Closure of the Privacy Incident

Closure is warranted after completion of the investigation of the incident, the issuance of external notification if appropriate, and the implementation of all suitable privacy and IT security mitigation measures. If a portion of one or more of these stages is ongoing, the incident cannot be closed. *See Appendix D, DHS Privacy Playbook: Handling Process Overview, for an overview and checklist for the incident closure process.*

The Component Privacy Officer/PPOC will update the Privacy Incident Report https://eoconline.dhs.gov to recommend incident closure, subject to review by the DHS Privacy Office, Director of Privacy Incidents and Inquiries, and DHS CIO. The Privacy Incident Report is closed unless DHS Privacy Office, Director of Incidents and Inquiries, or DHS CIO notifies the DHS SOC that the incident must remain open for review or further incident handling.

11. Annual Program Review of the Implementation of the PIHG

Members of the PIRT and other designated DHS senior officials are responsible for conducting an annual review of the implementation of the PIHG at the Departmental and Component levels. This annual program review occurs at the annual Core Management Group meeting. The review process includes:

- Review of Privacy Incidents that occurred during the preceding 12-month period and the manner in which they were handled;
- Identification of Privacy Incident handling procedures and practices that can be revised in order to strengthen DHS safeguards for PII;
- Identification and adoption of best practices that can be incorporated in the PIHG; and
- Examination of training programs pertaining to the implementation of the PIHG and safeguarding of PII.

The DHS CPO will chair the review process, and the DHS Privacy Office, Director of Privacy Incidents and Inquiries, will prepare the Annual Report for the Program Review of the PIHG, known as the Core Management Group Privacy Incident After Action Report.

12. Privacy and IT Security Awareness Training Concerning the Implementation of the PIHG and Responsibilities to Safeguard PII

Fairness requires that DHS personnel be informed and trained regarding their respective responsibilities relative to safeguarding PII, and the consequences and accountability for violation of these responsibilities. *See Appendix D, DHS Privacy Playbook: Handling Process Overview,* for an overview and checklist for the incident handling process. The DHS Privacy Office, DHS CIO, and DHS CISO continue to implement training programs that address these responsibilities.

Such programs will ensure that DHS employees (including managers) who use or who have access to DHS information resources receive training on their privacy and security responsibilities *before* they are permitted access to agency information and information systems. DHS requires an annual refresher training course to ensure that employees continue to understand their responsibilities**.** Such programs also remind supervisors of their responsibility to instruct, train, and supervise employees on safeguarding PII.

Component Heads must ensure that all individuals with authorized access to PII and their supervisors annually sign a document clearly describing their responsibilities.

Privacy Incident Handling Guidance

Appendices

Revised January 26, 2012

Homeland Security

TABLE OF CONTENTS

Appendix A: List of Acronyms

C&A	Certification and Accreditation
CFO	Chief Financial Officer
CFR	Code of Federal Regulations
CHCO	Chief Human Capital Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMG	Core Management Group
CONOPS	Concept of Operations
CPO	Chief Privacy Officer
CSIRC	Computer Security Incident Response Center
CSO	Chief Security Office
DAA	Designed Accrediting Authority
DHS	Department of Homeland Security
EOP	Executive Office of the President
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FOUO	For Official Use Only
FTC	Federal Trade Commission
GAO	Government Accountability Office

GSA	General Services Administration
HSPD	Homeland Security Presidential Directive
ISSM	Information Systems Security Manager
IT	Information Technology
MD	Management Directive
NIST	National Institute of Standards and Technology
OCC	Office of the Chief Counsel
OGC	Office of General Counsel
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PIHG	Privacy Incident Handling Guidance
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIRT	Privacy Incident Response Team
PM	Program Manager
PPOC	Privacy Point of Contact
PTA	Privacy Threshold Analysis
SOC	Security Operations Center
SP	Special Publication
SSA	Social Security Administration

SSL	Secure Socket Layer
SSN	Social Security number
TSA	Transportation Security Administration
URL	Uniform Resource Locator
U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team
VPN	Virtual Private Network

Appendix B: Authorities

The DHS information security and privacy programs are based upon public laws, external guidance, and internal DHS guidance.

Public Laws and U.S. Code

- The Privacy Act of 1974, 5 U.S.C. § 552a, provides privacy protections for records containing information about individuals (i.e., citizens and legal permanent residents) that are collected and maintained by the federal government and are retrieved by a personal identifier. The Act requires agencies to safeguard information contained in a system of records.
- The E-Government Act of 2002 (Public Law 107–347) requires federal agencies to conduct Privacy Impact Assessments (PIAs) for electronic IT systems that collect, maintain, or disseminate PII and to make these assessments publicly available.
- 5 CFR § 2635, Office of Government Ethics, *Standards of Ethical Conduct for Employees of the Executive Branch*, establishes standards of ethical conduct for employees of the Executive Branch of the United States Government.
- Section 222 of the Homeland Security Act of 2002 (Public Law 107-296) mandates that the Secretary of DHS appoint a senior official in the Department to assume primary responsibility for privacy policy.
- Homeland Security Presidential Directive (HSPD) 7 directs that each department and agency will identify critical infrastructure and key resources and provide information security protections that are "commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information."
- The Federal Information Security Management Act of 2002 (FISMA) directs that a program for detecting, reporting, and responding to security incidents be established in each department. FISMA also requires the establishment of a central federal information security incident center. The US-CERT center was established within DHS in 2003.

Office of Management and Budget Directives

- OMB Circular A-130 specifies that federal agencies will "[e]nsure there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats."
- OMB Memorandum M-06-15 (M-06-15), *Safeguarding Personally Identifiable Information* (May 22, 2006) reiterates and emphasizes agency responsibilities under law and policy to appropriately safeguard sensitive PII and train employees regarding their responsibilities for protecting privacy.

- OMB Memorandum M-06-16 (M-06-16), *Protection of Sensitive Agency Information* (June 23, 2006) requires agencies to implement encryption protections for PII being transported and/or stored offsite.
- OMB Memorandum M-06-19 (M-06-19), *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments* (July 12, 2006) requires agencies to report all incidents involving PII to US-CERT within one hour of discovery of the incident.
- OMB Memorandum M-06-20 (M-06-20), *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* (July 17, 2006) requires agencies to provide updated information on the agency's privacy management program (including incident response).
- OMB's Memorandum *Recommendations for Identity Theft Related Data Breach Notification* (September 20, 2006) outlines recommendations to agencies from the President's Identity Theft Task Force for developing agency planning and response procedures for addressing PII breaches that could result in identify theft.
- OMB Memorandum M-07-16 (M-07-16), *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007) identifies existing procedures and establishes several new actions agencies should take to safeguard PII and to respond to Privacy Incidents.

Other External Guidance

- FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems*, February, 2004 establishes standards to be used by all federal agencies to categorize all information collected or information systems maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels.

Internal Guidance

- DHS Management Directive (MD) 0480.1, *Ethics/Standards of Conduct*, March 1, 2003.
- DHS Management Directive (MD) 4900, *Individual Use and Operation of DHS Information Systems/Computer*, undated.
- DHS Management Directive (MD) 11042.1, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, January 6, 2005.
- DHS Privacy Policy Guidance Memorandum 2007-02, *Use of Social Security Numbers at the Department of Homeland Security*, June 4, 2007.
- DHS Privacy Office's *Handbook for Safeguarding Sensitive Personally Identifiable Information*, January 19, 2011.
- DHS Management Directive (MD) 4300A, *DHS Sensitive Systems Policy*, January 20, 2011.
- DHS Management Directive (MD) 047-01, *Privacy Policy and Compliance*, July 7, 2011.

Appendix C: Illustrations of Privacy Incidents

Definition of Privacy Incident

A **Privacy Incident** is defined by DHS as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users have access or potential access to personally identifiable information (PII) in usable form, whether physical or electronic, or where authorized users access PII for an unauthorized purpose. The term encompasses both **suspected and confirmed incidents** involving PII.

Privacy Incident handling requirements apply to all federal information and information systems in an unclassified environment, including "information in both electronic and paper format, personal and PII, and information maintained in a system of records as defined by the Privacy Act." See M-07-16.

Definition of Personally Identifiable Information

Personally Identifiable Information (PII) is 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 United States citizen, legal permanent resident, or a visitor to the U.S. PII includes any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history.

Examples of PII include: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), Internet protocol (IP) addresses, biometric identifiers (e.g., fingerprints), photographic facial images, or any other unique identifying number or characteristic; and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual. See *Privacy Impact Assessments, The Privacy Office Official Guidance*, June 2010.

Definition of Sensitive Personally Identifiable Information

Sensitive Personally Identifiable Information is personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

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 names of employees with poor performance ratings.

All Sensitive PII must be designated as MODERATE or HIGH impact for purposes of incident handling.

Illustrations

The following examples demonstrate instances in which a Privacy Incident may occur. This list is not exhaustive and is intended for illustration purposes only.

Loss of Control

- Lost shipment: A package of paper personnel files and CD-ROMs containing a ***password-protected zip file*** of a personnel database is lost during shipment. The paper files contain Sensitive PII about 120 component employees who have recently separated or retired from federal service. These paper records include ***full names, dates of birth, SSNs, and financial information (including salary and bank information)***.
- Lost thumb drive: An employee reports a lost unencrypted thumb drive that contained a file ***listing the names, telephone numbers, and badge numbers of contractors*** working on a component project. The file was ***not encrypted nor was it password protected***.
- Lost laptop: An employee reports a lost laptop used to enter time and attendance. The amount of PII stored on the laptop is unknown, but it is assumed that ***employee names, ID numbers, grade and salary information, home addresses, and truncated SSNs*** are present. The hard drive of the laptop was ***not encrypted***, but any files on the hard drive could be ***password protected***. During the subsequent investigation, it is discovered that while no PII was present on the laptop hard-drive, the laptop did attempt to ***connect back to the component's network***.

Compromise

- Three systems are hacked into, potentially making available the ***names, SSNs, and biometric information, including photographs and fingerprints***, of 26,000 employees, contractors, and retirees. There is no conclusive evidence regarding whether the data was compromised.
- A supervisor reports that a paper file is missing from her desk. The file contains employee evaluations which included ***names, SSNs, and performance ratings*** belonging to employees under her supervision.

Unauthorized Disclosure

- A document containing internal recommendations for ***grade level promotions and award bonuses*** for several employees assigned to agency headquarters is posted on the Component's intranet.
- An employee disposed of boxes containing sensitive information in a dumpster; the boxes contained a ***user password*** for a sensitive information technology (IT) pilot program, as well as copies of ***completed Standard Form (SF)-86 forms which contained SSNs, criminal history information and sensitive information about dependents***.
- A glitch on the Component's internet web page allows unauthorized read-only access to a database containing ***benefits information*** on 3,000 individuals.
- Documents containing the ***name, weight, height, eye and hair color*** of several new employees were mistakenly faxed from one component's security office to a government agency that was not authorized to receive the information.

Unauthorized Acquisition

- An employee reports that he inadvertently acquired access to five other employees' ***government credit card numbers and Personal Identification Numbers*** (PIN) located on the travel vouchers in the component's Travel Management System.
- An employee finds a box of documents outside of a storage closet with sensitive files containing the ***names, credit reports, authorization files, and signatures*** of several department employees under investigation for abuse of their government credit cards.
- A keylogger program was installed on an employee's unencrypted DHS laptop, allowing the ***capture of login and password information***.

Unauthorized Access (Internal and External)

- A contractor who misused administrator privileges gained unauthorized access to a procurement system and posted sensitive information on ***contract bids, government procurement card numbers, and tax identification numbers*** on the Component's internet web site, exposing an unknown amount of PII.

  An unknown person gained unauthorized access to a component field office. This intruder installed malicious software in the system that caused the transfer of files containing ***names, home addresses, salaries, and bank account numbers*** of 1700 individuals.

Appendix D: DHS Privacy Playbook: Handling Process Overview

This checklist provides the critical steps to be performed in the handling of a Privacy Incident. **Upon detection, DHS personnel must immediately report ALL suspected and confirmed incidents involving PII. DHS must officially report the incident to the U.S.-Computer Emergency Response Team (US-CERT) within one hour of notice to the DHS Chief Information Security Officer (CISO).**

DHS personnel must expedite reporting to ensure compliance with the mandatory OMB one-hour requirement. The incident handler must prioritize the activities identified in the following Process Overview as circumstances warrant.

Handling Process Overview

Reporting (Section 4)		
	DHS personnel detect incident that may involve PII.	
	DHS personnel notify Program Manager (PM) of suspected or confirmed incident. If PM is not available, DHS personnel contact Component Help Desk.	
	PM evaluates facts and determines whether an incident involving PII may have occurred.	
	PM makes preliminary report to Component IT Security Entity (e.g., Component Information Systems Security Manager [ISSM] / Component Security Operations Center [SOC] / Computer Security Incident Response Center [CSIRC]) if PM determines an incident may have occurred.	
	Component IT Security Entity consults with Component Privacy Officer/Privacy Office Point of Contact (PPOC) to confirm whether Privacy Incident has occurred and to coordinate incident handling.	
	Component Privacy Officer/PPOC or Component IT Security Entity enters report data into DHS EOC Online Incident Handling System at https://eoconline.dhs.gov.	
	DHS SOC analyst reviews report for accuracy and completeness and transmits report to US-CERT.	
	DHS SOC automatically transmits Privacy Incident Notification to the DHS Deputy Secretary, DHS CPO, DHS Privacy Office, Director of Privacy Incidents and Inquiries, DHS Chief Information Officer (CIO), DHS Deputy CIO, DHS CISO, and DHS Office of General Counsel (OGC) alerting DHS senior officials of report to US-CERT.	
	Component Privacy Officer/PPOC notifies DHS or Component Chief Financial Officer (CFO) of any Privacy Incident involving CFO Designated Financial Systems and government-issued credit cards.	
		DHS or Component CFO notifies the affected bank(s) of the incident when appropriate.
		The Component Privacy Officer/PPOC supplements the Privacy Incident Report to reflect the CFO's notification of the affected bank(s).
	Component Privacy Officer/PPOC notifies the DHS or Component CFO of any Privacy Incident involving individuals' bank account numbers used for direct deposit of credit card reimbursements, government employee salaries, or any benefit information.	
		The DHS or Component CFO notifies the Chief Human Capital Officer (CHCO) and the affected bank(s) of the incident when appropriate.
		DHS or Component CFO informs the Component Privacy Officer/PPOC of such notification.
		Component Privacy Officer/PPOC supplements the Privacy Incident Report to reflect the CFO's notification of affected bank(s).

	If an incident was initially reported as a Computer Security Incident and DHS SOC subsequently determines that the incident is also a Privacy Incident, the Component Privacy Officer/PPOC is notified. DHS SOC then notifies the DHS Deputy Secretary, DHS CPO, DHS CIO, DHS Deputy CIO, DHS CISO, and DHS OGC of the change in categorization. □ If a Privacy Incident impacts the security of an IT system, the PM refers to the DHS SOC CONOPS document for incident handling requirements.		
	If the Component Privacy Officer/PPOC determines that the incident affects additional components, the Component Privacy Officer/PPOC must notify components directly and document notification in Privacy Incident Report. In addition, the Component Privacy Officer/PPOC must notify DHS SOC.		
	DHS CIO notifies the DHS Chief Security Office (CSO) when the incident involves security-related issues affecting DHS personnel, property, facilities, and information.		
	US-CERT reports the incident to the appropriate external government entities.		
	Component Privacy Officer/PPOC responds to inquiries from US-CERT regarding the Privacy Incident.		
	Component Privacy Officer/PPOC supplements report at https://eoconline.dhs.gov as needed.		
Escalation to Determine Who Handles Incident and To Make Preliminary Recommendation Regarding Notification (Section 5)			
	Component Privacy Officer/PPOC conducts a risk analysis of the incident and documents the analysis in the Privacy Incident Report in the DHS EOC Online Incident Handling System.		
	Component Privacy Officer/PPOC consults with the Component IT Security Entity if the incident impacts the security of a DHS IT system.		
	Once the Privacy Incident has been reported to the DHS SOC, the Component Privacy Officer/PPOC immediately evaluates the context of the incident and the PII that was potentially or actually lost or compromised.		
		Component Privacy Officer/PPOC identifies the type of risk involved in the incident.	
			The Component Privacy Officer/PPOC evaluates whether the data elements constitute the type of information that may pose a risk of identity theft (e.g., types include: (1) SSN; or (2) name, address, or telephone number combined with: (a) any government-issued identification number; (b) biometric record; (c) financial account number; or (d) any additional specific factor that adds to the personally identifying profile of a specific individual; (3) date of birth, password, and mother's maiden name; or (4) Sensitive PII, such as SSN, Alien Registration Number, driver's license or state identification number, passport number, financial account number, citizenship or immigration status, or medical information. □ If the Component Privacy Officer/PPOC neither suspects nor confirms that identity theft is implicated, then the Component Privacy Officer/PPOC proceeds with the evaluation of the five factors determining the likely risk of harm. □ If identity theft is implicated, the Component Privacy Officer/PPOC creates a plan that is tailored to the nature and scope of the risk. This may involve convening a specialized PIRT.
		Component Privacy Officer/PPOC evaluates the five factors to determine the likely risk of harm posed by the Privacy Incident: ☐ The nature of the data elements involved; ☐ The number of individuals affected; ☐ The likelihood the PII is accessible and usable; ☐ The likelihood the Privacy Incident may lead to harm; ☐ The ability to mitigate the risk of harm.	
	Component Privacy Officer/PPOC assigns an impact level of low, moderate, or high to each risk factor.		

		The likely risk of harm is LOW when the risk of identity theft or other harm is unlikely (e.g., the compromise of the PII could not lead to identity theft or other risk of harm; the PII has been recovered and determined that there was no access or distribution of information; the PII was encrypted in accordance with DHS Policy for Laptop Computer and Other Mobile Computing Devices and validated by the National Institute of Standards and Technology [NIST]).	
			The likely risk of harm is MODERATE or HIGH when criminal activity is suspected or confirmed. • Component Privacy Officer/PPOC, in coordination with Component SOC or DHS SOC Government Watch Officer, will ensure external notification of law enforcement for incidents that do not impact physical security; such notification should be handled in consultation with the DHS CPO. • If criminal activity impacts physical security, the Component Privacy Officer/PPOC, in coordination with Component SOC or DHS SOC Government Watch Officer, will ensure consultation and reporting with the Component CSO; Component CSO will determine whether contacting internal or external law enforcement is necessary. • Notification and involvement of internal or external law enforcement must be documented in the Privacy Incident Report. All Sensitive PII must be designated as MODERATE or HIGH impact.
	Component Privacy Officer/PPOC recommends who should handle the incident (i.e., Component Privacy Officer/PPOC or specialized PIRT) for purposes of investigation, notification, mitigation, and closure.		
		Privacy Incidents with a LOW potential impact do not create a reasonable risk of harm and can be handled with minimum resources by the Component Privacy Officer/PPOC. Therefore, the Component Privacy Officer/PPOC will be responsible for handling Low-Impact Privacy Incidents, with guidance, as needed, from the DHS Privacy Office.	
		If the incident meets or exceeds the reasonable risk of harm standard, its potential will be moderate or high. The likely risk of harm for an incident in which criminal activity is suspected or confirmed is MODERATE or HIGH. Incidents involving Sensitive PII are always designated as MODERATE or HIGH impact. The Component Privacy Officer/PPOC will use their best judgment in determining who would comprise the PIRT to handle a Moderate-Impact incident occurring at the Component level. A specialized PIRT may be convened when the *potential impact* of the Privacy Incident occurring at the Component level is MODERATE according to Section 5.2. See Section 1.4.11 when considering enhancing the PIRT. A specialized PIRT may be convened when the *potential impact* of the Privacy Incident is HIGH according to Section 5.2, or when the *potential impact* of the incident is MODERATE but occurred at DHS Headquarters. The PIRT members will provide advice and assistance as needed to address the incident.	
	If the incident involves government-issued credit cards, individuals' bank account numbers used for direct deposit of credit card reimbursements, government employee salaries, or any benefit information, or CFO Designated Financial Systems, the Component Privacy Officer/PPOC determines whether the DHS or Component CFO should be included if a specialized PIRT is convened.		
	DHS CIO notifies DHS CSO when the incident involves security-related issues affecting DHS personnel, property, facilities, and information.		
	Component Privacy Officer/PPOC makes a preliminary recommendation as to whether notification is warranted		
		Component Privacy Officer/PPOC recommends notification when there is a reasonable risk of harm and the decision will not lead to the overuse of notification.	

		Notification must be consistent with the needs of law enforcement, national security, and any measures necessary for DHS to determine the scope of the incident, and if applicable, restore the reasonable integrity of the data system.
	Component Privacy Officer/PPOC identifies the steps DHS should take to mitigate the risk of harm.	
Mitigation (Section 6)		
Component Privacy Officer/PPOC works in consultation with the Component IT Security Entity, specialized PIRT (if convened), and PM to prevent or minimize any consequent harm.		
PM gathers, secures, and documents evidence of the incident.		
PMs collaborate with Component Privacy Officer/PPOC and Component IT Security Entity regarding containment measures.		
Component IT Security Entity and Component Privacy Officer/PPOC manage and contain the incident.		
Component IT Security Entity and Component Privacy Officer/PPOC implement actions to correct and prevent further risks stemming from the incident.		
Component Privacy Officer/PPOC secures paper records, if applicable.		
Component IT Security Entity and Component Privacy Officer/PPOC identify and mitigate exploited vulnerabilities.		
Component IT Security Entity removes malicious code or compromised or inappropriate materials from the network (including intranet) and/or Internet.		
Component IT Security Entity returns affected systems to an operationally ready state and confirms that the affected systems are functioning normally.		
Component Privacy Officer/PPOC restores security measures protecting paper information, if applicable.		
Component IT Security Entity and Component Privacy Officer/PPOC consider countermeasures as dictated by the nature and sensitivity of the PII, including but not limited to: ☐ Notification of affected individuals, the public, and other government entities (Section 8); ☐ Offering credit monitoring services to mitigate the misuse of the PII and identify patterns of suspicious behavior; ☐ Removal of information from an Internet or intranet page; ☐ Notification of the DHS CPO, DHS OIG, DHS CSO, and DHS OGC if criminal activity is suspected or confirmed and consultation to determine whether law enforcement should be notified; and ☐ Notification of the affected bank for incidents involving credit cards or bank accounts (Sections 4 and 5).		
Component IT Security Entity and Component Privacy Officer/PPOC document all implemented mitigation measures in the Privacy Incident Report.		
Investigation [PIRT members, Component Privacy Officer/PPOC, or Component IT Security Entity serve as investigators unless or until a lead investigator is designated] (Section 7)		
	Investigators limit internal notifications and access to individuals who have a legitimate need to know.	
	Investigators review what has occurred: ☐ Document the investigation and gather all information necessary to describe and respond to the incident. ☐ Review the Privacy Incident Report submitted to US-CERT and identify what additional information is necessary. ☐ Confirm what personal information is lost or at risk. ☐ Identify what steps have been taken to reduce the risk of harm.	
	Investigators develop a plan of action.	
		If a specialized PIRT is convened, clearly define investigative responsibilities of each PIRT member based upon the capability, expertise, and authority of the member in order to ensure proper handling of the Privacy Incident and to avoid duplicative efforts.
		Identify the lead investigator for a particular Privacy Incident. It should be someone who is trained

		or familiar with incident response procedures, and the complexities involved with the potential loss or compromise of PII: • If no specialized PIRT is convened, the lead investigator will report to the Component Privacy Officer/PPOC or Component IT Security Entity. If the incident involves physical security, the lead investigator may report to the Component CSO. If a Moderate-Impact Privacy Incident is involved, the lead investigator may also report to the DHS OIG and DHS OGC. • The lead investigator should consult with Component OCC or DHS OGC before initiating investigation into issues involving the handling of evidence and chain of custody.
		Investigators follow the DHS internal incident handling procedures: • Identify what further steps must be taken to formulate any further response by DHS. • Identify information resources that have been affected and identify additional resources that might be affected. • Estimate the current and potential technical impact (e.g., data, database, system or network) of the incident. • Back up the system in accordance with the standards and procedures set forth in DHS 4300A Sensitive Systems Handbook.
	Investigators adhere to standard investigation procedures.	
		Investigators create and maintain a complete record of the investigation.
		Investigators protect and preserve all evidence as follows: • Consult with Component OCC or DHS OGC to address issues involving the handling of evidence and chain of custody. • Take precautions to prevent destruction or corruption of evidence that may be needed to support criminal prosecution. • Identify and properly secure all evidence to maintain its validity in court.
		Investigators create and maintain a chain of custody log of everyone who has access to the evidence. Investigators keep a record of the individuals who have touched each piece of evidence. The record should include the date, time, and locations of where the evidence is stored.
		The Component Privacy Officer/PPOC, in coordination with Component SOC or DHS SOC Government Watch Officer will ensure external notification of law enforcement for incidents that do not impact physical security. If criminal activity impacting physical security is suspected, the Component Privacy Officer/PPOC, in coordination with Component SOC or DHS SOC Government Watch Officer, will ensure consultation and reporting with the Component CSO, who will determine whether contacting law enforcement is necessary. Notification and involvement of internal or external law enforcement must be documented in the Privacy Incident Report.
		Protect the chain of custody of the backup data. Store the data in a secure location.
	Law enforcement will consult with the lead investigator and other PIRT members as warranted. For incidents where criminal activity is suspected or confirmed, the lead investigator will consult with law enforcement, DHS OIG, and the Component CSO regarding the closure of the investigation.	
	Investigators review events and actions at the conclusion of the incident and make recommendations to the DHS CPO, DHS SOC and PIRT members regarding any suggested changes in the DHS technology and incident handling plan.	
	Upon completion of the investigation, the Component Privacy Officer/PPOC updates the Privacy Incident Report at https://eoconline@dhs.gov to indicate the closure of the investigation, subject to review by the DHS CPO and DHS SOC.	
Notification (Section 8)		

	Once the Component Privacy Officer/PPOC has completed the Privacy Incident Report, a decision to publicly release information may be reached through collaboration with the Component Head and specialized PIRT if convened.
	If notification is warranted, the Component Privacy Officer/PPOC, and specialized PIRT members, will assess how and when notification outside DHS should be given (e.g., timing of notification, source of notification, means for providing notification, and who should receive notification).
	If the Component Privacy Officer/PPOC determines that external notification is warranted, the following occur: ☐ Component Privacy Officer/PPOC prepares the notification letter and the draft press release, if any, and consults the Component Head if necessary. ☐ On occasion, the DHS CPO or DHS Privacy Office, Director of Privacy Incidents and Inquiries, may need to coordinate with DHS Public Affairs Office to provide *reasonable advance internal notice* to DHS senior officials by email or voicemail of a notification decision before external notification is made. ☐ The Component Head, DHS CPO, DHS CIO and DHS Legislative Affairs Office will work closely to determine when notification of the incident should be provided to congressional oversight committee chairs. With respect to a High-Impact Privacy Incident, DHS Legislative Affairs Office and DHS Public Affairs Office 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.
	Component Privacy Officer/PPOC sends notification letter to affected third parties.
	Component Privacy Officer/PPOC may attach notification documents to the Privacy Incident Report in the DHS EOC Online Incident Handling System (e.g., External Notification Assessment, press release, notification letter to affected individuals).
Consequences and Accountability for Violation of Federal Laws, Regulations, or Directives, or DHS Policy (Section 9)	
	Component Privacy Officer/PPOC informs the Component Head when DHS personnel have failed to implement safeguards to protect PII, or when a Privacy Incident arose from a violation or potential violation by DHS personnel of applicable laws, regulations, policies, or directives governing the protection of PII.
	Component Heads take corrective and disciplinary actions when security or Privacy Incidents and violations occur and hold personnel accountable for intentional transgressions.
	Component Heads work with the Designated Agency Ethics Officials as well as the OIG, OGC, and CHCO in the event that the Privacy Incident arises from violations or potential violations of the ethics statutes or regulations.
	Component Privacy Officer/PPOC notifies the DHS OGC and Component OCC when DHS personnel (including employees, supervisors, and managers) fail to implement safeguards to protect PII or when a Privacy Incident arose from a violation or potential violation by DHS personnel of applicable laws, regulations, policies, or directives governing the protection of PII.
	DHS OGC or Component OCC consults with the Component Privacy Officer/PPOC or other specialized PIRT members, Component Head, and CHCO on legal issues pertaining to disciplinary or corrective action.
	Component Privacy Officer/PPOC may document in the Privacy Incident Report any violation(s) or potential violation(s) that caused or contributed to, in part or whole, the Privacy Incident without naming personnel.
	CHCO maintains a record of all disciplinary or corrective actions taken against DHS personnel that arise out of a Privacy Incident.
Closure of the Privacy Incident (Section 10)	
	Component Privacy Officer/PPOC and Component IT Security Entity update the incident report at https://eoconline.dhs.gov to recommend incident closure, subject to review by the DHS Privacy Office,

	Director of Privacy Incidents and Inquiries, and DHS CISO.
	Incident report is closed unless DHS Privacy Office, Director of Incidents and Inquiries, or DHS CIO notifies DHS SOC that the incident must remain open for review or further incident handling.

Appendix E: Escalation Risk Assessment

(To be completed by the Component Privacy Officer/PPOC)

Incident Number:	**Prepared by:**	**Position:**
Date:	**In Consultation with:**	**Position:**
Component:	**Program:**	

The Component Privacy Officer/PPOC may use this form as a framework for analyzing the likely risk of harm posed by the Privacy Incident. The Component IT Security Entity should be consulted during this process if the incident impacts the security of a DHS IT system.

Caution: Do NOT disclose actual PII on this form (e.g., SSN, name, etc.). This assessment may be modified as the factual basis for the incident develops during incident handling.

Section 1: Brief Description of the Circumstances Surrounding the Potential Loss of PII	
Specify data elements potentially at risk.	☐ Name ☐ Date of birth ☐ Mailing address ☐ Telephone number ☐ SSN ☐ Alien Registration Number ☐ Email address ☐ Zip code ☐ Account numbers ☐ Certificate/license numbers ☐ Vehicle identifiers ☐ URLs ☐ Biometric identifiers ☐ IP addresses ☐ Other (Specify):
Indicate whether the incident is suspected or confirmed.	
Explain how the information was potentially compromised. State the media (e.g., paper, email, shared drive) used and identify to whom the information was disclosed.	

Specify mitigation steps that have already been taken to reduce risk of harm.	

Section 2: Identify Type of Risk

To identify if the Privacy Incident involves identity theft concerns, check the appropriate boxes. Indicate whether the incident involves any of the following data elements:

- ☐ SSN
- ☐ Alien Registration Number
- ☐ Biometric Identifier (e.g., fingerprint, iris scan, voice print)
- ☐ Any government-issued identification number (e.g., driver's license or state identification number, passport number).
- ☐ Financial account number.
- ☐ A name, address, or telephone number, combined with:
  - ☐ Citizenship or immigration status.
  - ☐ Other data used by DHS to identify or authenticate an individual's identity, such as a fingerprint identification number (FIN) or Student and Exchange Visitor Information System (SEVIS) identification number;
  - ☐ Date of birth, password, or mother's maiden name.

This will help identify the type of risk involved. **If the incident does <u>not</u> involve data elements that implicate identity theft concerns, the identity theft risk is minimal and it is unlikely that further steps designed to address identity theft risks are necessary. If such data elements are <u>not</u> involved, use the impact levels set forth in Section 3 to assess the likely risk of harm in Section 3(b). Complete the table in Section 3(b) and then proceed to Section 4.**

If the incident <u>does</u> involve data elements that implicate identity theft concerns, immediately notify the DHS Privacy Office. The Component Privacy Office/PPOC in close consultation with the DHS OIG and DHS Privacy Office will prepare and complete the Escalation Risk Assessment. Use the impact levels set forth in Section 3 to assess the likely risk of harm in Section 3(b). Complete the table in Section 3(b), then proceed to Section 4.

Section 3(a): Standards for Analysis of Risk

Impact Levels Used for Categorization

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

(1) Could result in limited or no harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained; or

(2) Could have limited or no adverse effect on organizational operations or organizational assets.

The likely risk of harm is LOW for *de minimus* risks. *De minimus* risks include those instances in which the PII was inadvertently compromised but posed no reasonable risk of harm.

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

(1) Could result in significant harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained; or

(2) Could have a serious adverse effect on organizational operations or organizational assets; or

(3) The incident involves Sensitive PII (see PIHG Section 1.4.13).

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

(1) Could result in severe or catastrophic harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained; or

(2) Could have a severe or catastrophic adverse effect on organizational operations or organizational assets; or

(3) The incident involves Sensitive PII (see PIHG Section 1.4.13.)

Section 3(b): Analysis of Risk: Five Factors

Privacy Incidents That Pose Risk of Identity Theft

(Component Privacy Officer/PPOC Assesses the Level of Risk)

Type of Factor	Identify Risk Level (e.g., Low, Moderate, High) and Provide Brief, Specific Explanation
Nature of data elements involved	Consider the data elements in its context. Were the data elements compromised PII? Yes ☐ No ☐ (See Section 1) Explain:

Number of individuals affected	Is there a way to identify the number of the individuals impacted by the incident? (For example, is there a recent computer backup of all information or is there a hard copy of the information?) Yes ☐ No ☐ Identify the total number of affected individuals (if known): Explain how the identity of affected individuals is known.
Likelihood PII is accessible and usable	Is the information ☐ Electronic or ☐ Hardcopy? How difficult is it for an unauthorized person to gain access to protected information? Was it locked or secured? Yes ☐ No ☐ If secured, identify what physical or electronic protections for electronic or hardcopy, if any, apply. Summarize the risk of whether an unauthorized individual will know the value of the information and either use the information or sell it to others.
Likelihood incident may lead to harm	Will substantial harm, embarrassment, inconvenience, or unfairness occur from this loss? Yes ☐ No ☐ Explain why. Determine the likelihood the incident is the result of or could result in criminal activity. Focus on the way the loss or compromise of PII occurred. • Was it the result of a criminal act (e.g., PII stolen was targeted by a computer hacker)? Yes ☐ No ☐ • Is it likely to result in criminal activity? Yes ☐ No ☐ • Was the storage device, rather than the PII itself, the target of the theft? Yes ☐ No ☐ • Is there evidence that the compromised information is being used to commit identity theft? Yes ☐ No ☐ **NOTE: If the answer is yes to any of these questions, the Component Privacy Officer/PPOC should categorize the incident as either a Moderate- or a High-Impact Privacy Incident. A specialized PIRT may be convened for incident handling. Under these circumstances,**

	Component Privacy Officer/PPOC, in coordination with Component SOC or DHS SOC Government Watch Officer, will ensure external notification to law enforcement for incidents that do not impact physical security. Such notification should be handled in consultation with the DHS CPO. If criminal activity impacts physical security, the Component Privacy Officer/PPOC, in coordination with Component SOC or DHS SOC Government Watch Officer, will ensure consultation with the Component CSO. Component CSO will determine whether contacting internal or external law enforcement is necessary.
Ability to mitigate risk of harm	Please explain to what extent the component has the capabilities to take countermeasures. Does the incident involve government-issued credit cards? Yes ☐ No ☐ If so, has DHS notified the affected bank? Yes ☐ No ☐ Does the incident involve individuals' bank account numbers used for direct deposit of credit card reimbursements, government employee salaries, or any benefit payment? Yes ☐ No ☐ If so, has DHS notified the affected bank? Yes ☐ No ☐ Can DHS monitor and prevent attempts to misuse the affected information? Yes ☐ No ☐ Does the compromised information present a risk of new accounts being opened? Yes ☐ No ☐ If so, is incident monitoring appropriate (e.g., volume of persons affected or law enforcement evidence)? Yes ☐ No ☐ Would credit monitoring be more appropriate? Yes ☐ No ☐ Have appropriate law enforcement agencies been contacted to participate in the investigation of the incident? Yes ☐ No ☐ If so, state who has been contacted.

Section 4: Escalation Risk Assessment and Plan of Action by the Component Privacy Officer/PPOC		
Categorization of Privacy Incident	☐ Low ☐ Moderate ☐ High	Explain which factors were given greater weight and why. Explain complexity of incident. Analyze logistical challenges in handling incident. **Note: In an incident involving a risk of identity theft where there is likelihood that the incident is the result of or could result in criminal activity, then categorization should be at least moderate impact.**
Responsibility for Handling Incident	☐ Privacy Officer/PPOC for Component experiencing incident ☐ Specialized PIRT (based on their capability, expertise, and authority as needed)	
Suggested mitigation measures	Briefly explain what, if any, privacy and IT security controls can be implemented to mitigate the risks associated with incident. Briefly outline all other steps DHS should take to mitigate the risk of harm. Explain immediate mitigation steps taken (e.g., identify senior officials at DHS, law enforcement agencies or other institutions that should be notified; state containment measures that should be implemented).	
Recommendation: preliminary assessment of whether external notification is warranted	Based on the facts known at the time of escalation, make a preliminary recommendation whether external notification is necessary. **NOTE: The final decision regarding external notification will be made by Component Privacy Officer/PPOC in consultation with the Component Head if appropriate.** **If appropriate, notification should be provided without unreasonable delay following the discovery of a Privacy Incident, consistent with the needs of law enforcement and national security, and any measures necessary for DHS to determine the scope of the incident and, if applicable, to restore the reasonable integrity of the information system compromised.** **Prior to the issuance of external notification, reasonable advance notice to DHS senior officials must be given.**	

Appendix F: Identity Theft Overview

Overview of Identity Theft

Although a Privacy Incident may pose many types of harm, special attention must be given to the harm resulting from identity theft. Recovering from identity theft can be a lengthy, costly, and stressful process. It is essential that the incident handling plan be designed to minimize the damage caused by the loss or compromise of PII. Therefore, a Privacy Incident that raises identity theft concerns may necessitate a specialized PIRT.

In analyzing a Privacy Incident, the Component Privacy Officer/PPOC should evaluate whether the incident involves the type of information that poses a risk of identity theft, and review the nature of the data elements involved in the incident. Once the incident has been evaluated, the Component Privacy Officer/PPOC will create a plan that is tailored to the nature and scope of the risk.

Standards for Categorization of Privacy Incident Posing Risk of Identity Theft

The Preliminary Risk Analysis will be used to gauge the severity of the incident (i.e., likely risk of harm), which will determine who will handle the Privacy Incident on behalf of DHS. The results of this analysis will also be used as the basis for the decision of whether notification is warranted. *See Appendix E for the Escalation Risk Assessment* template.

The severity of the Privacy Incident will be categorized as low, moderate, or high in accordance with the standards set forth in Section 5.2 of this guidance. With respect to Privacy Incidents involving identity theft concerns, the following considerations also apply:

The likely risk of harm is LOW when the risk of identity theft or other harm is unlikely. Low-Impact Privacy Incidents should not lead to identity theft or other risk of harm such as embarrassment, inconvenience, or unfairness. LOW potential impact may include Privacy Incidents when:

- The compromise of the PII could not lead to identity theft or other risk of harm;
- The PII has been recovered and determined there was no access or distribution of information; or
- The PII was encrypted in accordance with DHS Policy for Laptop Computers and Other Mobile Computing Devices and validated by NIST.

The likely risk of harm is MODERATE or HIGH when the criminal activity is suspected or confirmed. Under these circumstances, the Component Privacy Officer/PPOC, in coordination with Component SOC or DHS SOC Government Watch Officer, will ensure external notification

to law enforcement for incidents that do not impact physical security. Such notification should be handled in consultation with the DHS CPO. If criminal activity impacting physical security is suspected, the Component Privacy Officer/PPOC, in coordination with Component SOC or DHS SOC Government Watch Officer, will ensure consultation with and reporting to the Component CSO. Component CSO will determine whether contacting internal or external law enforcement is necessary.

Sensitive PII results in a reasonably high risk of harm to the individual due to the sensitivity of the specific data elements. Incidents involving Sensitive PII are always designated as MODERATE or HIGH impact.

Escalation Risk Assessment

Consumer information is the currency of identity thieves, and perhaps the most valuable piece of information is the SSN. The SSN can be used to open new accounts and obtain credit or other benefits. Other information, such as account numbers, PINs, and passwords, are also valuable because they enable thieves to access existing consumer accounts. The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* (April 23, 2007)[1]

Nature of the Data Elements

If the Privacy Incident includes any of the following types of or combinations of Sensitive PII, the incident may pose a risk of harm to include identity theft:

- SSN
- Alien Registration Number
- Any government-issued identification number (e.g., driver's license or state identification number, passport number);
- Financial account number
- Biometric identifier (e.g., fingerprint, iris scan, voice print)
- A name, address, or telephone number, combined with:
  - Citizenship or immigration status;
  - Other data used by DHS to identify or authenticate an individual's identity, such as a fingerprint identification number (FIN) or Student and Exchange Visitor Information System (SEVIS) identification number;
  - Medical information;
  - Date of birth, password, or mother's maiden name

[1] http://www.idtheft.gov/reports/StrategicPlan.pdf.

All Sensitive PII must be categorized as MODERATE or HIGH.

See Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS at http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_spii_handbook.pdf.

Other Factors Influencing the Determination of Whether the Information Accessed Could Result in Identity Theft

When PII has been compromised, additional factors should be considered in determining whether the information accessed could result in identity theft. In determining the level of risk of identity theft, the agency should consider not only the data that was compromised, but all of the circumstances of the data loss, including:

- How easy or difficult it would be for an unauthorized person to access the PII in light of the manner in which the data elements were protected;
  - For example, information on a computer laptop that is adequately protected by encryption is less likely to be accessed, while paper copies are unprotected.
- The means by which the loss occurred, including whether the incident might be the result of a criminal act or is likely to result in criminal activity;
  - For example, the risk of identity theft is greater if data was stolen by a thief who was targeting the data (such as a computer hacker), rather than if the information was inadvertently left unprotected in a public location. In some cases of theft, the circumstances might indicate that the data-storage device, such as a laptop left in a car rather than the information itself, was the target of the theft. An opportunistic criminal may exploit information once it comes into his/her possession, and this possibility must be considered when determining a response, along with the recognition that risks vary with the circumstances.
  - In making this assessment, law enforcement may need to be consulted. If criminal activity is suspected or confirmed, the Component Privacy Officer/PPOC should categorize the incident as either Moderate- or High-Impact, and must notify the DHS SOC and DHS CSO (if incident impacts physical security), and a specialized PIRT may be convened for handling.
- The ability of the component to mitigate identity theft;
  - The ability of the component or other affected entities to monitor for and prevent attempts to misuse the compromised information can be a factor in determining the risk of identity theft. For example, if the information relates to disaster relief beneficiaries, monitoring the beneficiary database for duplicate requests may signal fraudulent activity. Likewise, alerting financial institutions in cases of a Privacy Incident involving financial account information can allow them to monitor or close the compromised accounts.
- Evidence that the compromised information is being used to commit identity theft or has been sold.

Considering these factors together should permit the Component Privacy Officer/PPOC to determine where the identity-theft risk occurred. This assessment should guide the component's additional actions. If it is determined that an identity theft risk is present, DHS should tailor its response, which may include advice to those potentially affected, services the agency may provide to those affected, and public notice, to the nature and scope of the risk presented.

Actions that Individuals Can Routinely Take

Steps that individuals can take to protect themselves depend upon the type of information compromised. In notifying potentially affected individuals about steps they can take following an incident, components should focus on the steps that are relevant to the particular circumstances, which include the following:

- Affected individuals can contact their financial institution to determine whether their account(s) should be closed. This option should be taken when financial account information such as credit card or bank account information is part of the incident.
- Affected individuals can monitor their financial account statements, and immediately report any suspicious or unusual activity to their financial institution or the credit reporting agencies. Suspicious activities can include:
    - Inquiries from companies the affected individual has not contacted or done business with;
    - Purchases or charges on the affected individual's accounts that he or she did not make;
    - New accounts that the affected individual did not open or changes to existing accounts that he or she did not make;
    - Bills that do not arrive as expected;
    - Unexpected credit cards or account statements that arrive in the mail;
    - Denials of credit for no apparent reason; and
    - Calls or letters about purchases that the affected individual did not make.

- First, affected individuals may wish to consider placing a fraud alert in their credit file to let creditors know to contact them before opening a new account in their name. The individual simply needs to call any one of the three credit reporting agencies at the phone numbers listed below.
    - Equifax: 1-800-525-6285
    - Experian: 1-888-397-3742
    - TransUnion: 1-800-680-7289

  They should:
    1. Request that a fraud alert be placed on their account; and
    2. Order a free credit report from the agency once they receive notice that the alert has been placed.

We recommend that the affected individual request a free credit report from each agency with a 4-month interval between requests. In other words, make a request to one agency, wait 4 months, then submit a request to the next agency, and so on. The affected individual should continue to do so for a period of 12-24 months.

- Second, when the affected individual receives their credit reports, they should review them carefully for accounts that they did not open or for inquiries from creditors that they did not initiate. Also, they should review their PII for accuracy. If the individual sees anything that they do not recognize or understand, they should immediately call the credit agency at the number on the report.

- Third, if the affected individual finds any suspicious activity on their credit reports, they should promptly file a report with their local police office and the Federal Trade Commission (FTC). Suspicious activities could include the following:
    - Inquiries from companies they have not contacted or done business with;
    - Additional addresses, dates of birth, or names on their report that do not belong to them;
    - Purchases or charges on their accounts they did not make; and
    - New accounts they did not open or changes to existing accounts they did not make.
- Affected individuals may consider placing a credit freeze on their credit file at no cost. This option is most useful when the incident includes information that can be used to open a new account, such as SSNs.
- Affected individuals can review resources and file an identity theft complaint at the Federal Trade Commission's (FTC) identity theft web site, www.ftc.gov/idtheft, or can call to speak with a counselor at 1-877-438-4338.
- Components need to be aware that a public announcement of the Privacy Incident can allow criminals engaged in fraud to use various techniques to deceive affected individuals into disclosing their credit card numbers, bank account information, SSNs, passwords, or other sensitive personal information.
- For deployed members of the military, including the National Guard, individuals should consider placing an active duty alert in their credit file. The Active Duty alert is placed in the credit file for a period of one year and allows for the individual to designate a power of attorney to deal with any issues that come up. Such active duty alerts serve a similar function as initial fraud alerts, causing creditors to be more cautious in extending new credit.

Appendix G: Sample Notification Letter

[Date]

Dear _____,

This letter is to inform you that **[Insert description of document, system, or device]** containing personally identifiable information (PII) about you was **[lost/stolen/compromised]** on **[Insert date of incident and/or detection of incident]**. We apologize for this **[loss/error]** and want to assure you that we are diligently working to prevent this situation from occurring again. **[Explain whether security controls like password-protection, encryption, etc., were used and what steps have already been taken to reduce the risk of harm]**. **[Describe actions taken by agency (e.g.., referred to external agency or local police) for investigation]**. Appropriate steps are being taken to mitigate the loss of your personally identifiable information and to protect against and prevent any further incidents.

As a precaution, you may wish to consider taking the following steps:

- First, you may wish to consider placing a fraud alert on your credit file to let creditors know to contact you before opening a new account in your name. Simply call any one of the three credit reporting agencies at the phone numbers listed below:
    - Equifax: 1-800-525-6285
    - Experian: 1-888-397-3742
    - TransUnion: 1-800-680-7289

    You should:

    1. Request that a fraud alert be placed on your file; and
    2. Order a free credit report from the agency once you receive notice that the alert has been placed.

    We recommend that you request a free credit report from each agency with a 4-month interval between requests. In other words, make a request to one agency, wait 4 months, then submit a request to the next agency, and so on. You should continue to do so for a period of 12-24 months.

- Second, when you receive your credit reports, review them carefully for accounts that you did not open or for inquiries from creditors that you did not initiate. Also, review your PII for accuracy. If you see anything that you do not recognize or understand, you should immediately call the credit agency at the number on the report.

- Third, if you find any suspicious activity on your credit reports, promptly file a report with your local police office and the Federal Trade Commission (FTC). Suspicious activities could include the following:
    - Inquiries from companies you have not contacted or done business with;
    - Additional addresses, dates of birth, or names on your report that do not belong to you;
    - Purchases or charges on your accounts you did not make;
    - New accounts you did not open or changes to existing accounts you did not make;
    - Bills that do not arrive as expected;
    - Unexpected credit cards or account statements;
    - Denials of credit for no apparent reason; and
    - Calls or letters about purchases you did not make.

For additional information on identity theft, you may wish to visit the FTC's Identity Theft web site at http://www.ftc.gov/idtheft/ or call their identity theft hotline at 1-877-438-4338.

Please be alert to any phone calls, emails, and other communications from individuals claiming to be from the Department of Homeland Security**, [Component Name],** or other official sources, asking for your personal information or asking to verify such information. This is often referred to as information solicitation or "phishing." **Neither DHS nor [Component Name] will contact you to ask for or to confirm your personal information.**

The officials and employees of the Department of Homeland Security take our obligation to serve our citizens very seriously, and we are committed to protecting the information with which we are entrusted. In response to incidents like this, and the increasing number of privacy incidents in the public and private sectors, the Department is continuously monitoring its systems and practices to enhance the security of personal and sensitive information.

We sincerely apologize for any inconvenience or concern this incident may cause you. If you have questions regarding this letter, please contact **[Insert POC Name]**, **[Insert Component & Position Title]**, at **[Insert Phone Number]** or **[Insert Email Address]**.

Sincerely,

[Name of Signing Official]
[Office of Signing Official]

NOTE TO COMPONENT PRIVACY OFFICER/PPOC

On occasion, the DHS CPO or DHS Privacy Office, Director of Privacy Incidents and Inquiries, may need to coordinate with DHS Public Affairs Office to provide *reasonable advance internal notice* to DHS senior officials by email or voicemail of a notification decision before external notification is made.

REMOVE THIS MESSAGE BEFORE DISTRIBUTION

Appendix H: Sample Press Release

[DATE]

FOR IMMEDIATE RELEASE

[COMPONENT NAME]
[COMPONENT LOGO]

[COMPONENT]OPENS INVESTIGATION INTO **[BRIEF DESCRIPTION OF PRIVACY INCIDENT]**

WASHINGTON - The **[Component Name]** announced today that it has opened an investigation into **[Type of Incident & Method of Potential PII Compromise]**. **[Explain circumstances of incident and involvement of third parties (e.g., package mailing companies, local police, etc)].**

The **[Insert Component or office name]** is completely committed to safeguarding personally identifiable information (PII). Investigators from **[Component Name]** will assess whether policies or procedures should be modified to prevent similar incidents from occurring and to reduce the risk to PII. In the interim, **[Component Name]** has sent letters to all persons who are potentially affected by the Privacy Incident, notifying them of the incident and stating that all necessary actions are being taken to protect the individuals involved.

Persons affected by the Privacy Incident may contact **[Point of Contact]** at **[(_) - _____]**. Media inquiries should be directed to the DHS Public Affairs Office at **[( ) -]**.
###

[Short Summary of Component Mission]

View this document online **[URL]**
[Component] Public Affairs
[Component Website URL]

NOTE TO COMPONENT PRIVACY OFFICER/PPOC

On occasion, the DHS CPO or DHS Privacy Office, Director of Privacy Incidents and Inquiries, may need to coordinate with DHS Public Affairs Office to provide *reasonable advance internal notice* to DHS senior officials by email or voicemail of a notification decision before external notification is made.

REMOVE THIS MESSAGE BEFORE DISTRIBUTION