Privacy Incident Handling Guidance

Version 2.1

September 10, 2007

1. 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.

TABLE OF CONTENTS

2. Introduction

2.1. Purpose

The Department of Homeland Security (DHS) has a duty to safeguard personally identifiable information (PII) in its possession and to prevent the breach of PII in order to maintain the public's trust in DHS. The Privacy Incident Handling Guidance (PIHG) serves this purpose by informing DHS organizations, employees, senior officials, and contractors of their obligation to protect PII and by establishing procedures delineating how they must respond to the potential loss or compromise of PII. The PIHG also provides for individual accountability to create an incentive for compliance, thus ensuring the effective implementation of the guidance.

PIHG establishes DHS policy and procedures that DHS personnel must follow upon the detection or discovery of a suspected or confirmed incident involving PII. 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. An incident involving this type of information is known as a Privacy Incident. *See Appendix A for an Illustration of Privacy Incidents*.

OMB requires agencies to report all Privacy Incidents to the United States Computer Emergency Readiness Team (US-CERT) within 1 hour of discovering the incident, as mandated by OMB Memorandum 06-19, entitled *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 12, 2006, (M-06-19), and OMB Memorandum M-07-16, entitled *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* May 22, 2007 (OMB M-07-16); *see also Appendix B for the for the Privacy Incident Report Template*. The 1 hour time requirement commences when the DHS Chief Information Security Officer (DHS CISO) is notified of the incident.

OMB M-07-16 further delineates the appropriate reporting, handling, and notification procedures in the event a Privacy Incident occurs. It establishes two strict reporting timelines. First, M-07-16 mandates that personnel report a Privacy Incident as soon as practicable. OMB M-07-16 also requires the Department to report the Privacy Incident to US-CERT within 1 hour of notification to the DHS CISO. The memorandum also clarifies that PII and information systems where information resides should generally be categorized as either Moderate-Impact or High-Impact for implementing minimum baseline security requirements and controls. Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems.* Finally, it recommends minimum requirements for agency policies detailing the responsibilities of individuals authorized to access PII.

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

2.2. Scope

The PIHG applies to all DHS personnel 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, *Sensitive Systems Handbook*.

2.3. 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, including the following:

- 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.
- 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."
- 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.
- OMB Memorandum 06-15, *Safeguarding Personally Identifiable Information*, May 22, 2006, (M-06-15) reiterates and emphasizes agency responsibilities under law and policy to appropriately safeguard sensitive PII and train employees regarding their responsibilities for protecting privacy.
- OMB's Memorandum entitled, *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 06-16, *Protection of Sensitive Agency Information*, June 23, 2006 (M-06-16), requires agencies to implement encryption protections for PII being transported and/or stored offsite.
- OMB Memorandum 06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 12, 2006 (M-06-19), requires agencies to report all incidents involving PII to US-CERT within one hour of discovery of the incident.
- OMB Memorandum 06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, July 17, 2006 (M-06-20) requires agencies to provide updated information on the agency's privacy management program (including incident response) as part of the FY2006 FISMA report to OMB.
- OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007 (M-07-16) identifies existing procedures and establishes several new actions agencies should take to safeguard PII and to respond to Privacy Incidents.
- The President's Identity Theft Task Force drafted *Combating Identity Theft: A Strategic Plan*, April 23, 2007, a comprehensive strategic plan for steps the federal government can take to combat identity theft with recommended actions that can be taken by the public and private sectors. The report is available at www.idtheft.gov.
- The Privacy Act of 1974, 5 U.S. Code (U.S.C.) § 552a, provides privacy protections for records containing information about individuals (i.e., citizen, legal permanent resident, and visitor) 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.
- 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.
- 5 Code of Federal Regulations (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.
- DHS Management Directive (MD) 0480.1, *Ethics/Standards of Conduct*, March 1, 2003.

2.4. Definitions

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

2.4.2. Awareness, Training, and Education – Includes (1) awareness programs for training that changes organizational attitudes toward realization of the importance of security and the adverse consequences of its failure; (2) a training purpose, which is to teach people the skills that will enable them to perform their jobs more effectively; and (3) education that is more in-depth than training, targeted for security professionals and those whose jobs require expertise in automated information security. (National Institute of Standards and Technology [NIST], Special Publication [SP] 800-18, *Guide for Developing Plans for Federal Information Systems,* February 2006).

2.4.3. Computer Security Incident – An incident is a 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,* January 2004).

2.4.4. Control – The 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).

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

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

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

2.4.8. 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 and the Paperwork Reduction Act; OMB Circular A-130(6)(n), *Management of Federal Information Resources,* November 28, 2000).

2.4.9. 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. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (1) requires the use of such equipment; or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. 40 U.S.C. § 1401. The term "information technology" does not include national security systems as defined in the Clinger-Cohen Act of 1996 (40 U.S.C. § 1452); OMB Circular A-130; and 40 U.S.C. §1452.

2.4.10. Personally Identifiable Information – 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.

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 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, Official Guidance*, DHS Privacy Office. Personal information refers to 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.

2.4.11. 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, and for an other than authorized purpose, have access or potential access to PII in usable form, whether physical or electronic. The term encompasses both **suspected and confirmed incidents** involving PII which raise a reasonable risk of harm (see section 2.4.13).

2.4.12. Privacy Incident Response Team (PIRT) – A group of DHS officials at the Departmental level or at the Component level responsible for handling Privacy Incident investigation, mitigation, and notification, with oversight by the DHS Chief Privacy Officer (CPO). See OMB M-07-16 and OMB's Memorandum entitled, *Recommendations for Identity Theft Related Data Breach Notification*, September 20, 2006. Each PIRT is a standing team of officials organized in advance that will handle Privacy Incidents for the Component or for the

Department. Each team will include officials responsible for administering operational, privacy, and security programs. Its membership will also include legal counsel, the inspector general, law enforcement, and public and legislative affairs. Each PIRT member will provide assistance with incident handling based on their capability, expertise, and authority as warranted by the circumstances of the incident. 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.

Departmental-level PIRT (D-PIRT) refers to a standing group of DHS senior officials that is designated in advance to handle: (1) a High-Impact Privacy Incident; or (2) a Moderate-Impact Privacy Incident that occurred at DHS Headquarters. D-PIRT will be chaired by a senior DHS official and will include the following officials or qualified designees or representatives from the following offices:

- DHS Deputy Secretary
- DHS CPO
- DHS Chief Information Officer (CIO)
- DHS Office of General Counsel, General Law Division (OGC-GLD)
- DHS Office of Inspector General (OIG)
- DHS Chief Security Officer (CSO)
- DHS Public Affairs Office
- Office of Legislative and Inter-Governmental Affairs
- Management Directorate
- DHS Chief Financial Officer (CFO)
- Component IT Security Entity (e.g., Information Systems Security Manager (ISSM), Computer Security Incident Response Center (CSIRC), SOC for the Component)
- Component Privacy Office 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-level PIRT (C-PIRT) refers to a standing group of officials from the affected Component that is designated in advance to handle on behalf of the Component a Moderate-Impact Privacy Incident occurring at the Component level. Each DHS Component will have a C-PIRT, which will be chaired by the Component Privacy Office/PPOC, and will include the following officials or qualified designees or representatives from the following offices:

- Component Head

- Senior official(s) from the Component
- Component Privacy Office/PPOC
- Component CIO
- Component Office of Chief Counsel
- DHS OIG
- Component IT Security Entity (e.g., ISSM, CSIRC, SOC for the Component)
- Communications office representative for the Component
- Legislative and inter-governmental affairs office for the Component
- Management Office for the Component
- Component CFO
- PM for the program in which the incident occurred

2.4.13. Reasonable Risk of Harm – A likelihood that an individual may experience a substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

2.4.14. 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: social security number, driver's license 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. In addition, the context of the PII may determine whether the PII 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.

3. Roles and Responsibilities for Privacy Incident Handling

In 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 all formats (paper and electronic) and other media. DHS organizations and DHS personnel must understand and adhere to all relevant federal laws, regulations, and directives, and to Departmental directives and guidance.

3.1. DHS Personnel

Privacy Incident handling responsibilities are as follows:

- Attend periodic 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 PM is unavailable, contact the Help Desk for the Component.

3.2. Program Manager

Privacy Incident handling responsibilities are as follows:

- 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.
- Understand how to contact the Component Privacy Office/PPOC during normal working hours.
- Receive initial reports from DHS personnel regarding the possible detection of a Privacy Incidents.
- Consult with the Component Privacy Office/PPOC when necessary 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., 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 Office/PPOC and the Component IT Security Entity with the development of facts for the Privacy Incident Report.
- Provide advice, expertise, and assistance to PIRT (if convened) as warranted and in consultation with other members of the team.
- Assist with the investigation and mitigation of a Privacy Incident to the extent necessary.

3.3. Component Help Desk

Privacy Incident handling responsibilities are as follows:

- Recognize Privacy Incidents.
- Understand the Privacy Incident reporting process and procedures.
- Understand how to contact the Component Privacy Office/PPOC during normal working hours.

- Serve as an alternate to the PM by receiving initial reports of possible Privacy Incidents from DHS personnel where the PM is unavailable to receive the initial report or has a conflict of interest in handling the report.
- Make a brief preliminary Privacy Incident report to the Component IT Security Entity (e.g., ISSM, Component SOC, Component CSIRC); or if none is available, contact the DHS SOC directly.

3.4. Component Privacy Office and Privacy Point of Contact

Privacy Incident handling responsibilities are as follows:

- Ensure compliance with federal laws and Departmental policy safeguarding privacy in consultation with the DHS CPO and Component CIO
- Implement Privacy Awareness Training and Education under the direction of the DHS CPO.
- Understand the Privacy Incident handling process and procedures.
- Work in close consultation with the Component IT Security Entity, PM, and DHS CPO 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 CPO of the status of a potential Privacy Incident.
- Consult with the Component CIO concerning Privacy Incident handling.
- Work with the Component IT Security Entity to contain the Privacy Incident.
- Notify the DHS CFO of any Privacy Incident that involves government-authorized credit cards.
- Respond to inquiries from the US-CERT regarding Privacy Incident reports, and supplement the Privacy Incident Report in the DHS SOC Online Incident Handling System as further information is obtained.
- Consult with the DHS OIG on a case-by-case basis to determine the appropriate incident handling procedures for Moderate- and High-Impact Privacy Incidents.
- Assess the likely risk of harm posed by the Privacy Incident (e.g., low, moderate, or high impact) to determine, in collaboration with the DHS CPO, who should handle the investigation, notification, and mitigation of the incident.
- Handle the investigation, notification, and mitigation for Low-Impact Privacy Incidents and the Component IT Security Entity, with oversight as needed by the DHS CPO.
- Handle Moderate-Impact Privacy Incidents that occurred at the Component level in consultation with C-PIRT (if convened) and the Component IT Security Entity, with oversight as needed by the DHS CPO.
- Serve as the Chair of a C-PIRT once convened and act as liaison between DHS CPO and C-PIRT.

- Serve as a member of D-PIRT once convened and act as the liaison between D-PIRT and the Component affected by the Privacy Incident.
- Assist D-PIRT in handling the investigation, notification, and mitigation of High-Impact Privacy Incidents or Moderate-Impact Privacy Incidents that occurred at DHS Headquarters in consultation with the Component IT Security Entity.
- Draft documents as warranted by the Privacy Incident Handling process.
- Make joint decision with the Component Head regarding the propriety of external notification to affected third parties and the issuance of a press release in Low- and Moderate-Impact Privacy Incidents that occurred at the Component level.
- Provide internal notification to DHS organizations and to DHS senior officials as required by PIHG prior to the authorized public release of information related to privacy incidents.
- Make incident closure recommendations in consultation with PIRT (if convened), the Component IT Security Entity, and the DHS SOC.
- Maintain and update Component POC information for Privacy Incident handling.
- Prepare an annual report for the DHS CPO outlining the lessons learned from Privacy Incidents that occurred in the Component during the year, and identifying ways to strengthen Departmental safeguards for PII and improve Privacy Incident handling.

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

Privacy Incident handling responsibilities are as follows:

- Ensure that the DHS Information Security Program is both implemented and maintained throughout the Component.
- Consult and coordinate with the PM and the Component Privacy Office/PPOC regarding privacy issues affecting the security of information.
- Understand Privacy Incident handling process and procedures.
- Consult with the Component Privacy Office/PPOC and the PM in the preparation of the Privacy Incident Report in the SOC Online Incident Handling System for review by DHS SOC.
- Work with the Component Privacy Officer or PPOC to investigate and remediate aspects of Privacy Incidents that impact computer security.
- Provide advice, expertise, and assistance to PIRT (if convened) as warranted and in consultation with other members of the team.
- Provide Privacy Incident closure recommendations as necessary.

3.6. DHS Computer Security Incident Response Center

Privacy Incident handling responsibilities are as follows:

- Serve as a central repository and coordination point for Privacy Incidents within DHS SOC.
- Maintain a capability for responding to incidents 24 hours a day, 7 days a week, and maintain an open bridge line to provide rapid scalable access.
- Provide technical assistance, share security advisories with Components, and facilitate two-way sharing of information.
- Understand the Privacy Incident handling process and procedures.
- Assist the DHS SOC with detection and response of suspected and confirmed incidents possibly involving PII.

3.7. DHS Security Operations Center

Privacy Incident Handling responsibilities are as follows

- 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 IT Security Entity is unavailable.
- Understand the Privacy Incident handling process and procedures.
- Transmit Privacy Incident Reports to US-CERT within 1 hour of receipt from the Component IT Security Entity.
- Inform DHS senior official 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 Office/PPOCs, and the Component IT Security Entity as needed to facilitate Privacy Incident reporting, investigation, mitigation, and incident closure.

3.8. US-CERT

Privacy Incident handling responsibilities are as follows:

- Serve as the designated central reporting organization within the federal government and serve as the central repository for federal incident data.
- Communicate and coordinate with the Component Privacy Office/PPOC to obtain updates regarding Privacy Incident Reports.
- Notify appropriate authorities of the Privacy Incident.

3.9. DHS Chief Privacy Officer

Privacy Incident handling responsibilities are as follows:

- 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.
- Circulate 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 Office and PPOC regarding Privacy Incidents as warranted by the circumstances.
- Convene the D-PIRT to handle High-Impact Privacy Incidents or Moderate-Impact Privacy Incidents occurring at DHS Headquarters.
- Provide advice, expertise, and assistance to PIRT, where necessary, with the handling of Privacy Incidents in consultation with other members of the team.
- Review incident closure recommendations.
- Develop and implement Privacy Awareness Training and Education in coordination with the Component Privacy Office/PPOCs.
- Provide recommendations to the Chair of the D-PIRT and the Component Head in consultation with other members of the D-PIRT regarding the propriety of external notification to affected third parties and the issuance of a press release.
- Determine who will handle non-media-related inquiries concerning the status of Privacy Incidents or the implementation of this guidance.
- Examine monthly reports issued by US-CERT addressing the Privacy Incidents that were reported to US-CERT.
- Chair the review process of the implementation of the PIHG and prepare the Annual Report for the PIHG Program Review.

3.10. DHS Privacy Office

The Privacy Incident handling responsibilities are to develop, update, and maintain DHS Privacy Incident handling procedures.

3.11. DHS Chief Information Officer

Privacy Incident handling responsibilities are as follows:

- 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.
- Serve on the D-PIRT once convened.

- 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.
- Provide recommendations to the Chair of D-PIRT and the Component Head in consultation with other members of D-PIRT regarding the propriety of external notification to affected third parties and the issuance of a press release.
- Review incident closure recommendations.

3.12. Component Chief Information Officer

Privacy Incident handling responsibilities are as follows:

- Provide management direction to security operations.
- Serve as an advocate for privacy and computer security incident response activities in consultation with the DHS CIO, the DHS CPO, and the Component Privacy Office/PPOC.
- Serve on the C-PIRT for the Component (if convened).
- 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 4300, Attachment F.
- Provide recommendations to the Component Head in consultation with other members of the PIRT regarding the propriety of external notification to affected third parties and the issuance of a press release.

3.13. DHS Chief Information Security Officer

Privacy Incident handling responsibilities are as follows:

- Provide security oversight and information assurance for the DHS OneNet operations.
- Understand current issues that impact availability, confidentiality, and integrity of the network assets.
- Maintain awareness of security breaches or 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 remedial 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 the Privacy Incidents that were reported to US-CERT.

3.14. Departmental-level Privacy Incident Response Team

Privacy Incident handling responsibilities are as follows:

- Provide recommendations and assistance to the DHS CPO regarding the investigation, notification, and mitigation of High-Impact Privacy Incidents and Moderate-Impact Privacy Incidents occurring at DHS Headquarters.
- Coordinates through DHS SOC with external entities such as law enforcement, the Identity Theft Task Force, Social Security Administration (SSA), and the Executive Office of the President (EOP) during the investigation, notification, or mitigation stages of High-Impact Privacy Incidents as warranted or Moderate-Impact Privacy Incidents occurring at DHS Headquarters as warranted.
- Provide recommendations to the Component Head regarding the propriety of external notification to affected third parties and the issuance of a press release in High-Impact Privacy Incidents.
- 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.
- Assist the DHS CPO in the preparation of an annual Best Practices Report, consider the merits of the report, and release the report.

3.15. Component-level PIRT

Privacy Incident handling responsibilities are as follows:

- Provide advice and assistance to the Component Privacy Office/PPOC as needed regarding the investigation, notification, and mitigation of Moderate-Impact Privacy Incidents.
- Communicates and coordinates, through DHS SOC, with external entities such as law enforcement, the Identity Theft Task Force, SSA, and EOP during the investigation, notification, or mitigation stages as warranted.
- Provide recommendations to the Component Head in consultation with other members of the PIRT regarding the propriety of external notification to affected third parties and the issuance of a press release in Moderate-Impact Privacy Incidents.

3.16. Heads of Components

Privacy Incident handling responsibilities are as follows:

- Provide necessary resources or assistance to facilitate Privacy Incident handling.
- Provide advice, expertise, and assistance to the PIRT (if convened) as warranted and in consultation with other members of the team.
- Make joint decision with the Chair of the PIRT regarding the propriety of external notification to affected third parties and the issuance of a press release.
- Initiate and evaluate corrective and disciplinary action when Computer Security Incidents or Privacy Incidents and violations occur.

3.17. DHS Office of the Inspector General

Privacy Incident handling responsibilities are as follows:

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

3.18. DHS Office of the General Counsel, General Law Division and Component Office of Chief Counsel

Privacy Incident handling responsibilities are as follows:

- Provide advice, expertise, and assistance to PIRT, where necessary, and handle Privacy Incidents in consultation with other members of the team.

- Provide legal advice to the DHS CPO, the DHS CIO, the Component Privacy Office/PPOC regarding the potential for disciplinary action or corrective action against DHS personnel arising from a Privacy Incident.
- Provide recommendations to the Chair of PIRT and the Component Head in consultation with other members of PIRT regarding the propriety of external notification to affected third parties and the issuance of a press release.
- Advise the Chief Human Capital Officer (CHCO) on disciplinary actions taken.
- Review, revise, and comment on reports and corrective actions taken.

3.19. DHS Public Affairs Office and Communications Office for the Component

Privacy Incident handling responsibilities are as follows:

- Work with the Component Head and the Chair of 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.

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

Privacy Incident handling responsibilities are as follows:

- Consult and coordinate with the DHS CPO and the DHS CIO to determine when notification of the congressional oversight committee Chair of a Privacy Incident is necessary.
- Provide recommendations to the Chair of the PIRT and the Component Head in consultation with other members of the PIRT regarding the propriety of external notification to affected third parties and the issuance of a press release

3.21. DHS Management Office and Management Staff for the Component

Privacy Incident handling responsibilities are as follows:

- Provide recommendations to the Chair of the PIRT and the Component Head in consultation with other members of the PIRT regarding the propriety of external notification to affected third parties and the issuance of a press release.

3.22. Chief Human Capital Officer

Privacy Incident handling responsibilities are as follows:

- Work with the DHS CFO, Component Privacy Office, PPOC, or the PIRT as needed in Privacy Incidents involving individuals' bank account numbers to be used for the direct deposit of credit card reimbursements, government employee salaries, or any benefit information.

- Consult with the Component Head or designee(s) 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.

3.23. DHS Chief Security Officer

Privacy Incident handling responsibilities are as follows:

- Serve as the DHS Secretary's representative for all security-related matters.
- Advise the DHS Secretary on security-related issues affecting DHS personnel, property, facilities, and information.
- Provide support and guidance and coordinating with the DHS CIO to ensure that DHS IT systems are properly secured.
- Provide advice, expertise, and assistance to the PIRT with respect to Privacy Incidents that raise security-related issues affecting personnel, property, facilities, and information, and in consultation with other members of the team.

3.24. Component Chief Security Officer

Privacy Incident handling responsibility is as follows:

- Handle external notification to law enforcement where the Privacy Incident arises from criminal activity that impacts physical security.

3.25. DHS and Component Chief Financial Officers

Privacy Incident handling responsibilities are as follows:

- Coordinate with the Component Privacy Office/PPOC where the Privacy Incident involves government-authorized credit cards.
- Notify the issuing bank where the Privacy Incident involves government-authorized credit cards.
- Notify the bank or other entity involved where the Privacy Incident involves individuals' bank account numbers to be used for the direct deposit of credit card reimbursements, government salaries, travel vouchers, or any benefit payment.
- Serve as a member of the PIRT where CFO Designated Financial Systems are involved in the Privacy Incident.
- Provide recommendations to the Chair of the PIRT and the Component Head in consultation with other members of PIRT regarding the propriety of external notification to affected third parties and the issuance of a press release in Privacy Incidents involving CFO Designated Financial Systems.

3.26. DHS Deputy Secretary

Privacy Incident handling responsibilities are as follows:

- Ensure that DHS personnel and organizations understand and comply with all relevant federal laws, regulations, and directives, and Departmental regulations, policies, and guidance.
- Consult with DHS senior officials regarding the handling of Privacy Incidents as warranted by the circumstances.
- Provide recommendations to the Chair of the D-PIRT and the Component Head in consultation with other members of the D-PIRT regarding the propriety of external notification to affected third parties and the issuance of a press release.

3.27. DHS Secretary

Privacy Incident handling responsibilities are as follows:

- Ensure that DHS Personnel and organizations understand and comply with all relevant federal laws, regulations, and directives, and Departmental regulations and guidance.
- Consult with DHS senior officials regarding Privacy Incidents as warranted by the circumstances.

4. Overview of Privacy Incident Handling Procedures

The PIHG establishes the framework for identifying, reporting, and otherwise responding to Privacy Incidents in a timely, expeditious, and meaningful manner. *See Appendix C for the DHS Privacy Playbook: Handling Process Overview* for an overview of the incident handling process; *Appendix E for the Privacy Incident Handling Guidance Process Flows*. A quick and effective response in the event of a Privacy Incident is critical to efforts to prevent or minimize any consequent harm. An effective response necessitates disclosure of information regarding the incident to those individuals affected by it, as well as to persons and entities in a position to cooperate, either by assisting in notification to affected individuals or playing a role in preventing or minimizing harms from the breach. Internal notifications and access must be limited to those who have a legitimate need to know.

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

There are six stages of incident handling: (1) Reporting; (2) Escalation; (3) Investigation; (3) Notification; (4) Mediation; (5) Closure; and (6) Annual Program Review. 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 organizations must understand that they must also refer to the DHS CONOPS if a Privacy Incident also impacts the security of an IT system. In this situation, both the PIHG and the CONOPS would govern incident handling because the incident would constitute both a Privacy Incident and a Computer Security Incident.

5. Reporting Procedures

5.1. Reporting Standard

DHS personnel must inform the PM immediately upon discovery or detection of a Privacy Incident, regardless of the manner in which it occurred. *See Appendix C for the 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 and for an other than authorized purpose have access or potential access to PII in usable form, whether physical or electronic. The term encompasses both **suspected and confirmed incidents** involving PII which raise a reasonable risk of harm (see section 2.4.13).

DHS personnel must use 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 can likely would 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.

5.2. No Electronic/Paper Incident Distinction

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

5.3. Factual Foundation for the Report

5.3.1. Initial Report

As soon as DHS personnel discovers or detects a Privacy Incident, the duty to report the incident to the PM arises. 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 Office/PPOC and the Component IT Security Entity (e.g., ISSM, Component SOC, Component CSIRC).

5.3.2. Preliminary Written Report

The PM, or alternatively, 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 Office/PPOC and the Component IT Security Entity with the following information:

- Component name in which the incident occurred
- Name, phone number, and email address of the DHS personnel who discovered the incident
- Date and time of the incident and 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 definitions of personal information and PII for additional examples
  - Number of people potentially affected and the estimate or actual number of records exposed
  - Whether it was disclosed internally within DHS or externally
  - If external disclosure is involved, state whether it was disclosed to the federal government or to the public

If the Component IT Security Entity is not available to handle reporting for the incident, the report may be sent directly to DHS SOC for Privacy Incident reporting.

5.3.3. Privacy Incident Report in the DHS SOC Online Incident Handling System

Upon receipt of the Preliminary Written Report, the Component Privacy Office/PPOC and the Component IT Security Entity (e.g., 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 Office/PPOC or the Component IT Security Entity must open an incident report in the DHS SOC Online Incident Handling System at https://soconline.dhs.gov. *See Appendix B for Privacy Incident Template*. The circumstances of the incident will determine whether the Component Privacy Office/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, DHS phone number, and DHS email address of the DHS personnel who discovered the incident
- Incident category type—Privacy Incidents are always CAT 1 Incidents (Unauthorized Access) for purposes of US-CERT categorization and will be prioritized based on the nature and severity of the incident
- Date and time of incident, and 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 definitions of personal information and PII for additional examples)
    - 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
    - Whether it was disclosed internally, within DHS
    - Whether it was disclosed externally
    - If external disclosure is involved, state whether it was disclosed to the federal government or to the public
    - 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

5.4. Means of Reporting and Related Communications

A Privacy Incident may be reported by the Component via telephone, email, fax, or through the DHS CSIRC web site.

Once a Privacy Incident Report has been opened in the DHS SOC 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.

5.5. 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 following internal Privacy Incident reporting process.

5.5.1. 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 alternatively to the Help Desk for the Component. If the PM or Help Desk are unavailable, DHS personnel may report the incident directly to the Component IT Security Entity.

5.5.2. Tier 2 (PM or Help Desk)

The PM, or alternatively the Help Desk for the Component, will evaluate the incident with assistance from Component Privacy Office/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.

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

The Component Privacy Office/PPOC or the Component IT Security Entity (e.g., ISSM, Component SOC, or Component CSIRC) must immediately consult and evaluate the factual basis of the incident. The Component Privacy Office/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 Office/PPOC or the Component IT Security Entity open, prepare, and submit the written report of the incident in the DHS SOC Online Incident Handling System. If the Component IT Security Entity is unavailable, the DHS SOC will prepare and submit the Privacy Incident Report to meet the strict Privacy Incident reporting time requirements.

Upon the entry of the Privacy Incident Report in the DHS SOC Online Incident Handling System, DHS SOC will automatically send a Privacy Incident Notification to the DHS CPO, alerting the DHS CPO to the entry of the Privacy Incident Report in DHS SOC Online.

5.5.4. Tier 4 (DHS SOC)

The DHS SOC will review the Privacy Incident Report for factual sufficiency and will transmit the report to US-CERT within 1 hour of receiving the Privacy Incident Report from the Component IT Security Entity.

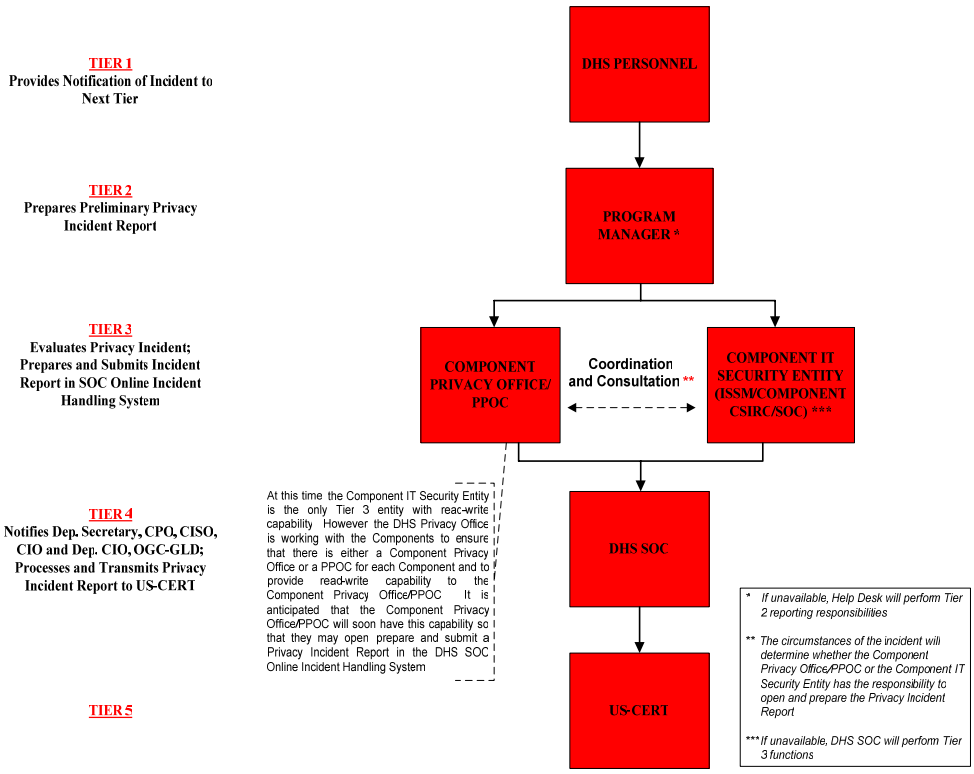


Diagram A: Reporting Process for Privacy Incidents

5.6. Supplementation of the Privacy Incident Report

After the DHS SOC has reported the Privacy Incident to US-CERT, the Component Privacy Office/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 but is not limited to factual information solicited by US-CERT or other information related to the escalation, investigation, notification, mitigation, or incident closure stages of incident handling. The PIRT or the Component Privacy Office/PPOC identifies and posts lessons learned in SOC Online Incident Handling System (https://soconline@dhs.gov).

5.7. Organizational Structure for Internal Notification of DHS Senior Officials

5.7.1. Notification of the DHS Deputy Secretary, DHS CPO, DHS CIO, DHS Deputy CIO, DHS OGC-GLD, and DHS CISO

When DHS SOC transmits the Privacy Incident Report to US-CERT, the DHS SOC will simultaneously and automatically issue a Privacy Incident Notification to the Deputy Secretary, DHS CPO, DHS CIO, DHS OGC-GLD, DHS Deputy CIO, and DHS CISO, alerting them of the transmission of the Privacy Incident report to US-CERT. 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.

5.7.2. 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 6.4.5 of this guidance.

5.8. Notification of External Entities

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

Within 1 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.

5.8.2. DHS CFO Notifies Issuing Bank

If the Privacy Incident involves government-authorized credit cards, the DHS 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 CFO must also notify the bank or other entity involved where the Privacy Incident involves individuals' bank account numbers to be used for the direct deposit of credit card reimbursements, government salaries, travel vouchers, or any benefit payment.

The DHS CFO will inform the Component Privacy Office/PPOC for the affected Component of such notification. The Component Privacy Office/PPOC will supplement the Privacy Incident Report to reflect the notification of issuing bank(s).

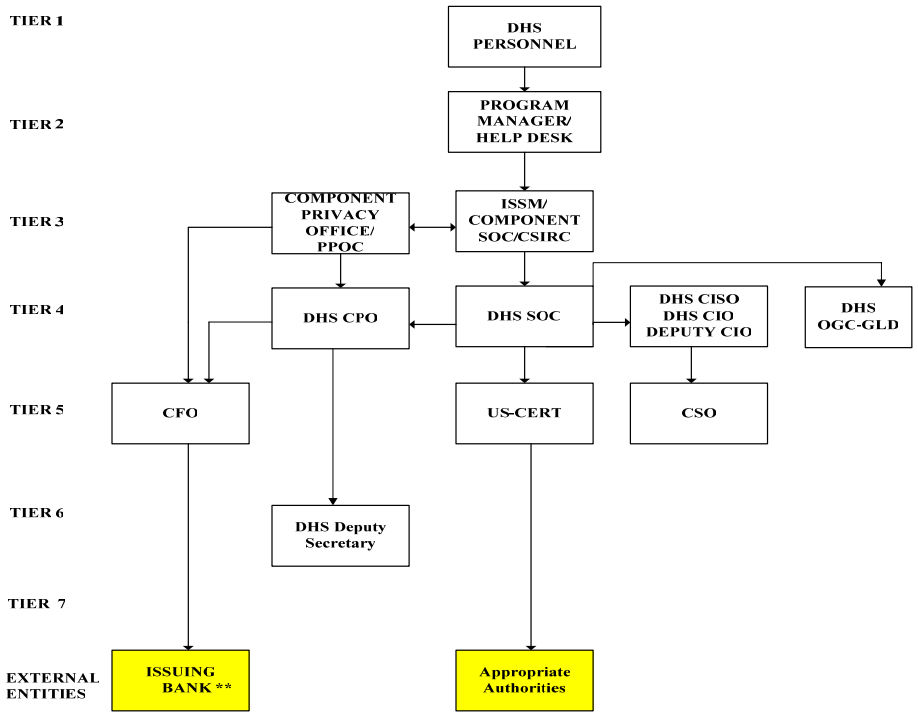


Diagram B: Organization Process for Notifying Senior DHS Officials and Notification of External Entities

6. 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. Under the guidance of the DHS Privacy Office, the Component Privacy Office/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 the DHS SOC, the Component Privacy Office/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 Office/PPOC must use its best judgment in using the following methodology:

1. Evaluate the five factors set forth in Section 6.3 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 Office, PPOC, C-PIRT or D-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 Office/PPOC will document its risk analysis in a report entitled, Escalation Risk Assessment, in the DHS SOC Online Incident Handling System. *See Appendix D for the Escalation Risk Assessment template*; *Appendix C for the DHS Privacy Playbook: Handling Process Overview* for an overview of the escalation process; *Appendix E for the Privacy Incident Handling Guidance Process Flows*. The Escalation Risk Assessment should be uploaded to the Privacy Incident Report in the DHS SOC Online Incident Handling System and sent via email to: the Deputy Secretary, the DHS Privacy Office at DHSPrivacyIncident@dhs.gov, the DHS CIO, and the DHS CISO.

If the Component Privacy Office/PPOC concludes that a C-PIRT should handle the remaining stages of the incident, the Component Privacy Office/PPOC should immediately convene the C-PIRT and send the Escalation Risk Assessment via email to its members.

If the Component Privacy Office/PPOC recommends that a D-PIRT handle the remaining stages of the incident, the Component Privacy Office/PPOC should immediately inform the DHS Privacy Office. A D-PIRT may be convened by the DHS Deputy Secretary, the DHS CPO, the DHS CIO, the DHS CISO, or other DHS senior officials as warranted by the circumstances. DHS senior officials will decide who will serve as the Chair of the D-PIRT for purposes of that particular the Privacy Incident. The Component Privacy Office/PPOC should promptly send the Escalation Risk Assessment to the members of D-PIRT via email.

The timing and sequence of events during escalation may vary from one incident to another. The exigencies of incident handling necessitate prompt decision-making concerning the escalation. Therefore, the Component Privacy Office/PPOC will be given a certain degree of flexibility and latitude. Escalation procedures may be performed in the order warranted by the circumstances. Escalation decisions that are verbal must be included in the Escalation Risk Assessment once it is prepared. It is essential, however, that the Escalation Risk Assessment be completed as soon as practicable because DHS officials will rely upon the assessment during incident handling.

6.1. The Initial Risk Analysis – Five Risk Analysis Factors

In developing the appropriate DHS response to a Privacy Incident, the Component Privacy Office/PPOC must first assess the likely risk of harm caused by the incident, and then assess the level of risk, with guidance, as needed, from the DHS Privacy Office. 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 as follows:

- The nature of the data elements involved (Section 6.3.1)
- The number of individuals affected (Section 6.3.2)
- The likelihood that PII is accessible and usable (Section 6.3.3)
- The likelihood that Privacy Incident may lead to harm (Section 6.3.4)
- The ability to mitigate the risk of harm (Section 6.3.5)

In analyzing a Privacy Incident, the first step that the Component Privacy Office/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 Office/PPOC will proceed with the assessment of the five factors with assistance, as needed from the DHS Privacy Office. If the Component Privacy Office/PPOC suspects or confirms that the Privacy Incident raises identity theft concerns, the Component Privacy Office/PPOC must immediately notify the DHS OIG and the DHS Privacy Office. The Escalation Risk Assessment will be performed by the Component Privacy Office/PPOC in close consultation with the DHS OIG and the DHS Privacy Office. *See Appendix D for the Escalation Risk Assessment*. Some Privacy Incidents require specialized attention because they pose a risk of identity theft. "The crime of identity theft occurs when an individual's identifying information is used by another without authorization in an attempt to commit fraud or other crimes." *Recommendations for Identity Theft Related Data Breach Notification*, September 20, 2006. The Component Privacy Office/PPOC should also refer to Section 6.6 of this guidance for substantive and procedural guidance concerning the handling of such incidents.

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

The form entitled *Escalation Risk Assessment* in Appendix D should be used to guide and document the risk assessment. The Component Privacy Office/PPOC should attach the completed form to the Privacy Incident Report in the DHS SOC Online Incident Handling System. The risk assessment will form the preliminary basis for determining whether notification is warranted.

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

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

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 a limited or no adverse effect on organizational operations or organizational assets.

Amplification of Low Likely Risk of Harm
The likely risk of harm is LOW for *de minimus* risks. A *de minimus* risk is a risk that is so small or insignificant that it should not be considered. *De Minimus* risks include those instances in which the PII was inadvertently compromised but the compromise poses no reasonable risk of harm. An example of a *de*

minimus risk is a situation in which a printed copy of a roster containing employee names and badge numbers is left on a printer for a limited time, promptly recovered by DHS staff, and returned to the owner.

A LOW likely risk of harm might include, for example, a Privacy Incident that might:

- Cause a degradation or reduction 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;
- Result in minor damage to organizational assets;
- Result in minor, limited, or no financial loss; or
- Result in minor harm to individuals.

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.

Amplification of Moderate Likely Risk of Harm

A MODERATE likely risk of harm might include, for example, a Privacy Incident that might:

- Cause a significant degradation or reduction 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;
- Result in significant damage to organizational assets;
- Result in significant financial loss; or
- Result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

Sensitive PII is always designated as MODERATE or HIGH impact.

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.

Amplification of High Likely Risk of Harm

A HIGH likely risk of harm might include, for example, a Privacy Incident that might:

- 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;
- Result in major damage to organizational assets;
- Result in major financial loss; or
- Result in experience severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Sensitive PII is always designated as MODERATE or HIGH impact.

6.3. Risk Analysis of Five Factors

6.3.1. 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 rolodex contains PII (name, phone number, etc.). In this context, the information probably would not be considered sensitive; however, the same information in a database of patients at a clinic which treats contagious disease 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: social security number, driver's license 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.

Examples of Risk Levels for Nature of Data Elements -- Examples	
Low	Compromise of a database containing the full names, mailing addresses, and job titles of subscribers to agency media alerts.

Moderate	Compromise of a database containing the full names, 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 of individuals receiving treatment for a contagious disease.

6.3.2. Factor Two: The Number of Individuals Affected

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 an agency should provide notification. See Section 8.2.8 in Notification for a discussion of the means of notification.

This factor, however, may directly impact the decision as to who should handle the Privacy Incident for purposes of investigation, notification, and mitigation. Where notification to a large number of affected individuals may be warranted, a PIRT should be convened to assist with logistical and substantive issues presented by the Privacy Incident.

6.3.3. Factor Three: The 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 agency. If the information is properly protected by encryption (an encryption method that has been validated by NIST), for example, the actual risk of compromise is low to non-existent.

The Component Privacy Office/PPOC will first need to assess whether the PII is at a low, moderate, or high risk of being compromised. The 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	Laptop was temporarily lost that contained the names, the last four digits of government-authorized credit card numbers of the federal employees in the Component who have purchasing authority; database containing PII was protected by NIST-validated encryption using the 128-bit encryption standard. The encryption key was not compromised. Laptop subsequently retrieved.
Moderate	Laptop was lost that contained the names, government-authorized credit card numbers. and Personal Identification Numbers (PIN) of the federal 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. Laptop was subsequently retrieved.
High	A hacker gained access to a database that contained the names, government-issued credit card numbers, and PINs of the federal employees in the Component who have purchasing authority; database containing PII was not encrypted. The information was protected only by a simple, single-case password and two-factor authentication was not used. Unauthorized charges subsequently appeared on employees' government credit card statements.

6.3.4. Fourth Factor: The Likelihood that the Privacy Incident May Lead to Harm to the Individual or to the Agency

6.3.4.1. 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.

6.3.4.2. Likelihood Harm Will Occur

The likelihood an incident may result in harm will turn 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, addresses, and badge numbers of persons who have completed DHS-required training.
Moderate	List containing the names, addresses, and badge numbers of persons under investigation for failure to complete DHS-required training.

High	List containing the names and addresses of persons who have provided information in a law enforcement investigation into drug smuggling.

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

- SSN
- A name, address, or telephone number, combined with:
  - Any government-issued identification number (such as a driver's license number);
  - Biometric record;
  - Financial account number, together with a PIN or security code, if a PIN or security code is necessary to access the account; or
  - Any additional, specific factor that adds to the personally identifying profile of a specific individual, such as a relationship with a specific financial institution or membership in a club
- Date of birth, password, or mother's maiden name
- Sensitive PII, such as SSN, driver's license number; financial account number; citizenship or immigration status; or medical information. All sensitive PII must be categorized as MODERATE or HIGH.

Under these circumstances, refer to Section 6.6 of this guidance for a discussion of Identity Theft.

6.3.5. Fifth Factor: The 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. Several factors should be considered. Appropriate countermeasures such as monitoring systems to identify patterns of suspicious behavior should be taken. For example, if the information relates to disability beneficiaries, monitoring a beneficiary database for requests for change of address 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 one agency's security office to a government agency that was not authorized to receive the information. The originating agency's security officer does not believe that 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 federal employees' government credit card numbers located on the travel vouchers in the agency's Travel Management System. The DHS CFO notifies the issuing banks of the incident and the accounts are immediately closed.
High	A document containing the names of a dozen employees in the Component receiving treatment for a contagious disease is posted on the Component's intranet for eighteen months. Upon learning of the incident, the Component immediately removes the posting from the intranet and informs the affected employees of the posting.

6.3.6. Balancing 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 Office/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. Where there is a range of risk levels attributed to the factors, the decision to provide notification should give greater weight to Factor Three (e.g., the likelihood the information is accessible and usable) and Factor Four (e.g., whether the Privacy Incident may lead to harm). Using this risk analysis, the Component Privacy Office/PPOC will then recommend to the DHS Privacy Office the appropriate severity of the incident.

Consider the following example and related risk analysis:

Balancing Risk Analysis Factors to Ascertain Severity of the Incident-- Examples	
Example	Laptop was temporarily lost that contained the names, credit card numbers, and PINs of the federal employees who have purchasing authority; database containing PII was protected by NIST-validated encryption using the 128-bit encryption standard. The laptop was retrieved shortly thereafter. The investigation revealed that the encryption key was not compromised and there was no access or distribution of information.
Analysis	The names, credit card numbers, and PINs 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 encrypted using NIST-validated encryption and the encryption key was not compromised. Therefore the data was not usable. There was also no evidence that the information was accessed or distributed. Therefore, Factor Three (e.g., the likelihood that the PII is accessible and useable) would have an impact level of **low**.

	Additionally, the fact that the laptop was promptly retrieved and tested to ensure that the information was neither accessed nor distributed. Therefore, Factor Five (e.g., the ability to mitigate the risk of harm) would have an impact level of **low**. Although the factors pertaining to the nature of the PII and the 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 (e.g., likelihood of compromise) and Factor Five (e.g., mitigation). Therefore, the **severity of the incident would be low**.

6.4. Determination of Who Will Handle the Privacy Incident

The Component Privacy Office/PPOC will determine who will handle the remaining stages of the Privacy Incident based upon the severity of the incident. This section delineates 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 provides a graphic display of the decision-making process for this section.

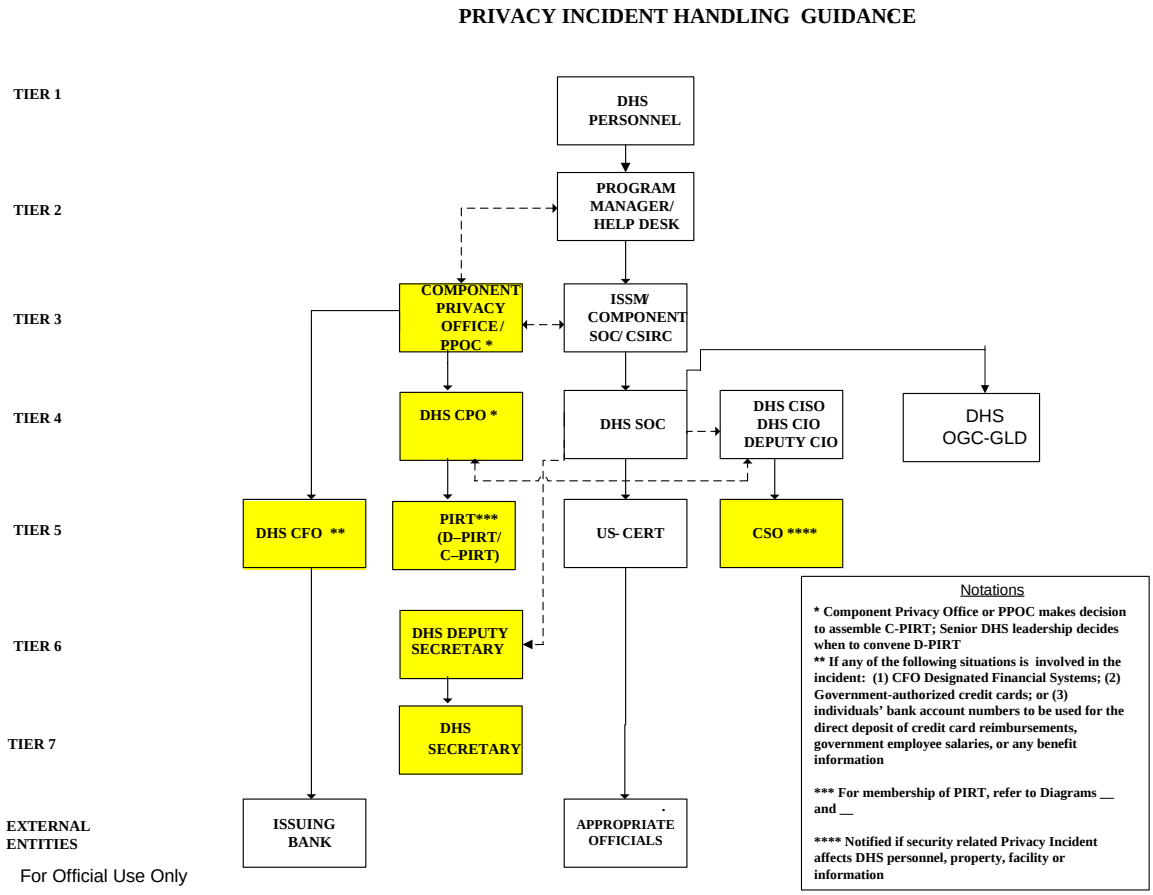


Diagram C: Process Flow for Escalation of Privacy Incident

6.4.1. 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 beyond those of the Component Privacy Office/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 incident handling such Low-Impact incidents. Therefore, the Component Privacy Office/PPOC will be responsible for handling Low-Impact Privacy Incidents, with guidance, as needed, from the DHS Privacy Office.

6.4.2. Privacy Incidents with a Moderate or High Potential Impact

If the incident meets or exceeds the reasonable risk of harm standard, its potential 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 Office or PPOC will use its best judgment in determining whether a C-PIRT should be convened handle a Moderate-Impact incident occurring at the Component level. See Diagram D for the composition of PIRT. A C-PIRT may be convened where the *potential impact* of the Privacy Incident occurring at the Component level is MODERATE according to Section 6.2 of this guidance. The following will apply:

- If a C-PIRT is convened to handle the incident, the Component Privacy Office/PPOC will:
    - serve as the Chair of C-PIRT;
    - promptly notify the C-PIRT members of the Privacy Incident; and
    - send the Escalation Risk Assessment to C-PIRT members via email.
- If a C-PIRT is not convened, the Component Privacy Office/PPOC will handle the incident with guidance as needed from the DHS Privacy Office.

The Component Privacy Office or PPOC may recommend that a D-PIRT handle the remaining stages of the incident. A D-PIRT may be convened where the *potential impact* of the Privacy Incident is HIGH according to Section 6.2 of this guidance or where the *potential impact* of the incident is MODERATE but occurred at DHS Headquarters. Where a D-PIRT is better suited to handle the response to an incident, the Component Privacy Office/PPOC should immediately inform the DHS Privacy Office. The DHS CPO and other DHS senior officials will then review the recommendation. The D-PIRT may be convened by the DHS Deputy Secretary, DHS CPO, DHS CIO, DHS OGC-GLD, DHS CISO, or other DHS senior officials as warranted by the circumstances. If a D-PIRT is convened, the DHS Privacy Office must perform the functions of the Component Privacy Office/PPOC with respect to incident handling and must send the Escalation Risk Assessment to the D-PIRT members via email. DHS senior officials will decide who will serve as the Chair of D-PIRT for purposes of that particular Privacy Incident. The PIRT members will provide advice and assistance as needed to address the incident.

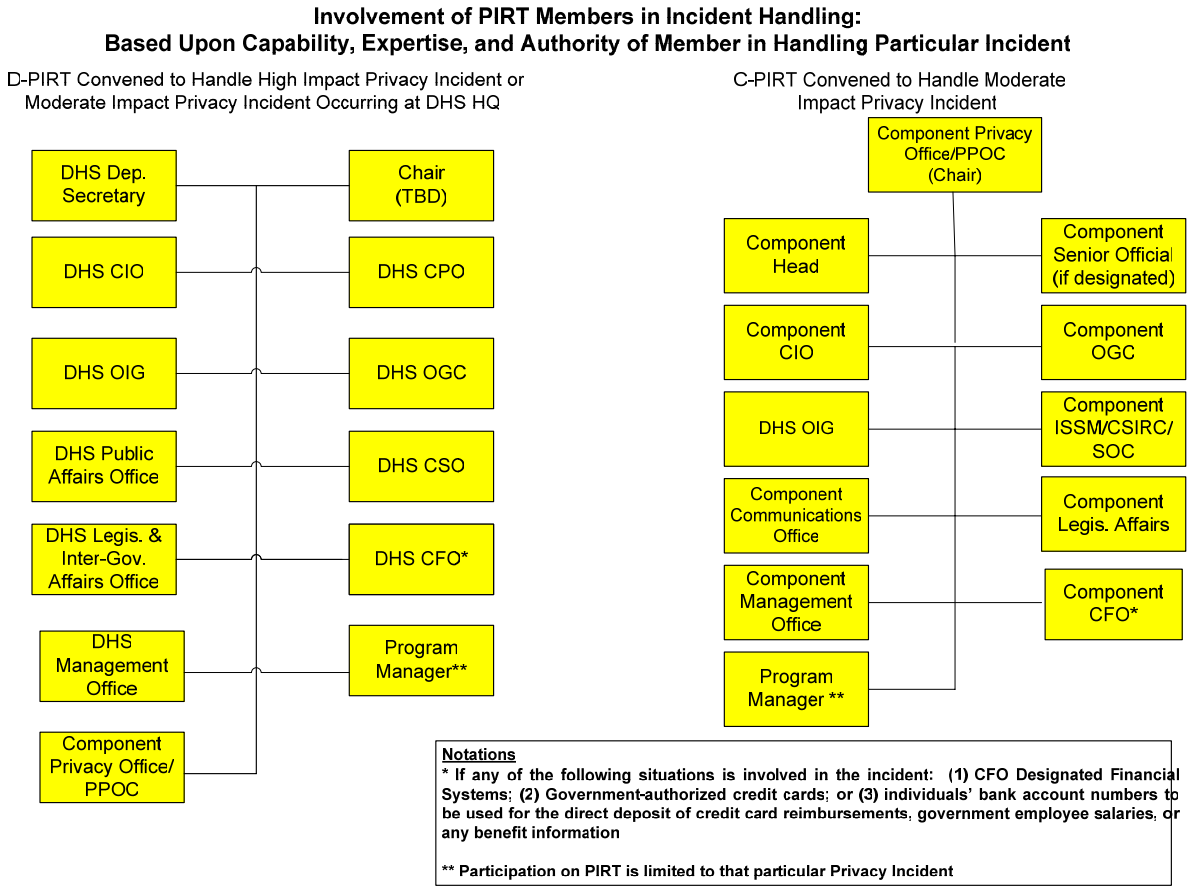


Diagram D: Composition of PIRT

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

The Component Privacy Office/PPOC will notify the DHS CFO of any Privacy Incident involving government-authorized credit cards. The DHS CFO will notify the issuing bank(s) of the incident where appropriate. The Component Privacy Office/PPOC will supplement the Privacy Incident Report to reflect the CFO's notification of the issuing bank(s).

Similarly, the Component Privacy Office/PPOC will notify the DHS CFO of any Privacy Incident involving individuals' bank account numbers to be used for the direct deposit of credit card reimbursements, government employee salaries, or any benefit information. The DHS CFO will notify the CHCO and the issuing bank(s) of the incident.

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. Component ISSMs and the Component Privacy Office/PPOC will ensure that Privacy Incidents related to CFO Designated Financial Systems are reported to the Component CFO.

If a PIRT is convened, the Component Privacy Office/PPOC will consult with the DHS CFO to determine whether the DHS CFO should be a member of the PIRT handling the Privacy Incident or whether the CFO for the Component experiencing the incident should be designated as a PIRT member.

Escalation steps taken must be documented in the Escalation Risk Assessment.

6.4.4. Special Circumstances Warranting Escalation to the DHS CSO

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

6.4.5. 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.

6.4.6. Preliminary Recommendation Regarding External Notification of Affected Individuals

In the Escalation Risk Assessment, the Component Privacy Office/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 where there is a reasonable risk of harm and the decision will not lead to the overuse of notification.

To determine whether notification of a breach is required, the agency should first assess the likely risk of harm caused by the breach and then assess the level of risk. Agencies 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 breach. Notification of those affected and/or the public affords 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 where notification could increase a risk of harm, the prudent course of action may be to delay notification while appropriate safeguards are put in place. Additionally, it is paramount 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.

When there is little or no risk of harm, notification might create unnecessary concern and confusion. The cost to individuals and businesses of responding to notices where 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 to them and fail to act even when risks are truly significant.

The Component Privacy Office/PPOC should apply these principles prudently in deciding whether notification is warranted. The Component Privacy Office/PPOC should exercise care in evaluating the benefit of notifying the public of Low-Impact Privacy Incidents. With respect to Moderate-- or High-Impact Privacy Incidents, notification should be recommended where it will provide affected individuals with the opportunity to take steps to help protect themselves from the consequences of the loss or compromise of PII, and where notification would align with the principles set forth in this section.

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

In the Escalation Risk Assessment, the Component Privacy Office/PPOC will explain whether and to what extent DHS may take countermeasures to mitigate the harm posed by the incident. Such steps may include, for example, eliminating unauthorized access to the PII, contacting the DHS OIG and law enforcement, notifying issuing banks, and monitoring accounts for unauthorized use. Refer to Section 9 for a discussion of mitigation.

6.6. Criteria for Evaluating Identity Theft

6.6.1. 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. “The crime of identity theft occurs when an individual’s identifying information is used by another without authorization in an attempt to commit fraud or other crimes.” *Recommendations for Identity Theft Related Data Breach Notification*, September 20, 2006. 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. The implications of the incident can extend beyond the scope of the data items that have been lost and can lead to additional unauthorized disclosures or financial losses.

To minimize the extent of the damage, DHS must take action as soon as possible. Therefore, the escalation of a Privacy Incident that raises identity theft concerns necessitates an expedited procedure and the full utilization of the relevant expertise of PIRT members.

In analyzing a Privacy Incident, the first step that the Component Privacy Office/PPOC should take is to evaluate whether the incident may involve the type of information that may pose a risk of identity theft, and review the nature of the data elements involved in the incident. If the

Component Privacy Office/PPOC suspects or confirms that the Privacy Incident raises identity theft concerns, the Component Privacy Office/PPOC must immediately notify the DHS OIG and the DHS Privacy Office. The Escalation Risk Assessment will be performed by the Component Privacy Office/PPOC in close consultation with the DHS OIG and the DHS Privacy Office. *See Appendix D for the Escalation Risk Assessment*. Upon completion of the Escalation Risk Assessment, the Component Privacy Office/PPOC will then distribute the assessment to other PIRT members. PIRT will promptly review the completed assessment and may provide comments to assist in assessing the likely risk of harm. PIRT will assist with crafting an incident handling plan that is tailored to the nature and scope of the risk presented.

6.6.2. 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 (e.g., likely risk of harm) which will, in turn, indicate who should 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 D 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 6.2 of this guidance. With respect to Privacy Incidents involving identity theft concerns, the following considerations also apply:

The likely risk of harm is LOW where 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 where:

- 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 Encryption and validated by NIST.

The likely risk of harm is MODERATE or HIGH where the criminal activity is suspected or confirmed. Under these circumstances, the Component Privacy Office/PPOC, in coordination with Component SOC or DHS SOC Security Technical Support 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 is suspected, the Component Privacy Office/PPOC in coordination with Component SOC or DHS SOC Security Technical Support Officer will ensure consultation and reporting with the Component CSO; Component CSO will determines whether to contact law enforcement (internal or external).

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.

6.6.3. Escalation Risk Assessment

Consumer information is the currency of identity theft, and perhaps the most valuable piece of information for the identity thief is the SSN. The SSN and a name can be used in many cases to open an account and obtain credit or other benefits in the victim's name. Other data, such as PINs, account numbers, 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*, at 13 (April 23, 2007))

6.6.3.1. Nature of the Data Elements

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

- SSN
- Name, address, or telephone number, combined with:
  - Any government-issued identification number (such as a driver's license number if the thief cannot obtain the SSN);
  - Biometric record;
  - Financial account number, together with a PIN or security code, if a PIN or security code is necessary to access the account; or
  - Any additional, specific factor that adds to the personally identifying profile of a specific individual, such as a relationship with a specific financial institution or membership in a club.
- Date of birth, password, or mother's maiden name
- Sensitive PII, such as SSN, driver's license number; financial account number; citizenship or immigration status; or medical information. All sensitive PII must be categorized as MODERATE or HIGH.

If this type of information is present, the data elements implicate identity theft concerns. The Component Privacy Office/PPOC will immediately notify the DHS OIG and the DHS Privacy Office. The Component Privacy Office/PPOC in close consultation with the DHS OIG and the DHS Privacy Office will evaluate the five risk analysis factors and complete the Escalation Risk Assessment together. The PIRT members will then review the assessment and may provide recommendations.

If the Privacy Incident does not involve this type of information, the risk of identity theft is minimal. It is unlikely that further steps designed to address identity theft risks are necessary.

6.6.3.2. Other Factors Bearing Upon the Determination Whether the Information Accessed Could Result in Identity Theft

Even where the PII has been compromised, various other 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 simply 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 was protected;
  - For example, information on a computer laptop that is adequately protected by encryption is less likely to be access, while "hard copies" of printed data are essentially 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) than if the information was inadvertently left unprotected in a public location. Similarly, in some cases of theft, the circumstances might indicate that the data-storage device, such as a computer 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 fashioning a response, along with the recognition that risks vary with the circumstances under which incidents occur.
  - In making this assessment, law enforcement may need to be consulted. If criminal activity is suspected or confirmed, the Component Privacy Office/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 PIRT must be convened for handling.
- The ability of the agency to mitigate the identity theft;
  - The ability of an agency 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 compromised information relates to disability beneficiaries, the agency can monitor its beneficiary database for requests for a change of address, which may signal attempts to misuse the information, and take steps to prevent the fraud. 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 actually being used to commit identity theft.

Considering these factors together should permit the Component Privacy Office, PPOC, DHS OIG and DHS Privacy Office to develop an overall sense of where the identity-theft risk created by the particular incident falls. That assessment, in turn, should guide the agency's further 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.

6.6.3.3. Mitigation: Reducing the Risk after Disclosure

While assessing the level of risk in a given situation, the agency should simultaneously consider options for reducing that risk. See also Section 9 for a discussion of mitigation measures. Certain options are available to agencies and individuals to help potential victims:

6.6.3.3.1. Actions that Individuals Can Routinely Take

The steps that individuals can take to protect themselves depend upon the type of information compromised. In notifying the potentially affected individuals about steps they can take following a data breach, agencies should focus on the steps that are relevant to those individuals' particular circumstances, which may include the following:

- Affected individuals may contact their financial institution to determine whether their account(s) should be closed. This option is relevant only when the financial account information is part of the breach.
- Affected individuals can monitor their financial account statements and immediately report any suspicious or unusual activity to their financial institution. Suspicious activities could include the following:
  - 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;
  - Denials of credit for no apparent reason; and
  - Calls or letters about purchases that the affected individual did not make.
- Affected individuals may request a free credit report from Equifax, Experian, and TransUnion.
- Affected individuals may place an initial fraud alert on credit reports maintained by the three major credit bureaus (e.g., Equifax, Experian, and TransUnion). This option is most useful when the breach includes information that can be used to open a new account, such as SSNs. After placing an initial fraud alert, individuals are entitled to a free credit report, which they should obtain beginning 2 to 3 months after the Privacy Incident, and review for signs of suspicious activity.
- For residents of states in which state law authorizes a credit freeze, affected individuals may consider placing a credit freeze on their credit file. This option is most useful when the breach includes information that can be used to open a new account, such as SSNs.
- For deployed members of the military, affected individuals could consider placing an active duty alert on their credit file. This option is most useful when the breach includes information that can be used to open a new account, such as SSNs. Such active duty

alerts serve a similar function as initial fraud alerts, causing creditors to be more cautious in extending new credit.

- Affected individuals could review resources provided on the Federal Trade Commission's (FTC) identity theft web site, www.ftc.gov/idtheft.
- Agencies should be aware that the public announcement of the Privacy Incident could itself cause criminals engaged in fraud, under the guise of providing legitimate assistance, to use various techniques to deceive individuals affected by the Privacy Incident into disclosing their credit card numbers, bank account information, SSNs, passwords, or other sensitive personal information.

6.6.3.3.2. Actions that DHS HQ Office and Components Can Take

If the breach involves government-authorized credit cards, the agency should notify the issuing bank promptly. If the breach involves individuals' bank account numbers to be used for the direct deposit of credit card reimbursements, government employee salaries, or any benefit payment, the Component Privacy Office/PPOC will notify the DHS CFO. See Section 6.4.3 of this guidance for the escalation procedure involving the DHS CFO. The DHS CFO will then notify the issuing bank.

Two other significant steps can offer additional measures of protection – especially for Privacy Incidents where the compromised information presents a risk of new accounts being opened – but will involve additional agency expense. First, technology can help analyze whether a particular data loss appears to be resulting in identity theft. This data breach analysis may be a useful intermediate protective action, especially where the agency is uncertain about whether the identity-theft risk warrants implementing more costly additional steps such as credit monitoring, or where the risk is such that agencies wish to do more than rely on the individual action(s) identified in the previous section.

Second, agencies may provide credit-monitoring services. Credit monitoring is a commercial service that can assist individuals in early detection of instances of identity theft; thereby allowing them to take steps to minimize the harm (although credit monitoring cannot guarantee that identity theft will not occur). A credit monitoring service typically notifies individuals of changes that appear in their credit report, such as creation of new account or new inquiries to the file. Agencies may wish to consult with OMB or FTC concerning the most current, available options for credit-monitoring services.

In deciding whether to offer credit monitoring services and type and length, agencies should consider the seriousness of the risk of identity theft arising from the Privacy Incident. Particularly important are whether incidents have already been detected, and the cost of providing the service. In addition, the agency should consider the characteristics of the affected individuals. Some affected populations may have more difficulty taking the self-protective steps described earlier.

Finally, notification to law enforcement is an important way for an agency to mitigate the risks faced by the potentially affected individuals. External notification to law enforcement where

criminal activity is suspected or confirmed should be handled by Component CSO and/or DHS CSO, depending on level and severity of criminal activity. The Component Privacy Office/PPOC will coordinate with Component SOC or DHS SOC Security Technical Support Officer in consultation with the DHS CPO. 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 enable the government to look for potential links, and to effectively investigate and punish criminal activity that may result from, or be connected to, the Privacy Incident. See Section 7 for the investigation procedure.

6.6.3.3.3. Providing Notice to Those Affected

The notification procedures set forth in Section 9 of this guidance govern the decision to provide external notification.

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; *see also the Privacy Incident Handling Guidance Process Flows*. The Component Privacy Office, PPOC, or Component IT Security Entity will coordinate the following investigation procedures unless or until a lead investigator is designated:

- Limit the internal notifications and access to those who have a legitimate need to know.
- Review what has happened:
  - Document the investigation and gather all information necessary to describe and address the incident.
  - Review the Privacy Incident Report submitted to US-CERT and identify what additional information, if any, 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 PIRT is convened, clearly delineate investigative responsibilities of each PIRT member based upon the capability, expertise, and authority of each PIRT 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 in or familiar with incident response procedures and the complexities involved with the potential loss or compromise of PII.
    - If no 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, however, the lead investigator must also report to the DHS OIG and DHS OGC-GLD.

        - If a D-PIRT is convened, depending upon the circumstances, the lead investigator will report to the Chair of the D-PIRT or his/her designee.
        - If a C-PIRT is convened, depending upon the circumstances, the lead investigator may report to the Chair of the C-PIRT or his/her designee.
        - The lead investigator should consult with Component OGC or DHS OGC-GLD before initiating investigation on issues pertaining to the handling of evidence and chain of custody.
    - Follow the DHS internal incident handling procedures:
        - Identify what further steps must be taken for the formulation of any further response by DHS.
        - Analyze the precedents and indications regarding computer security.
        - 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

- Adhere to standard investigation procedures:
    - Create and maintain a complete record of the investigation.
    - Protect and preserve all evidence.
        - Consult with Component OGC or DHS OGC-DHS to address issues pertaining to 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 Office/PPOC in coordination with Component SOC or DHS SOC Security Technical Support 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 is suspected, the Component Privacy Office/PPOC in coordination with Component SOC or DHS SOC Security Technical Support Officer will ensure consultation and reporting with the Component CSO; Component CSO will determines whether to contact law enforcement (internal or external).
    - Notification and involvement of 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 then consult with the lead investigator and other PIRT members as warranted. In incidents in which criminal activity is suspected or confirmed, the lead investigator will consult with law enforcement, the DHS OIG, and the Component CSO regarding the closure of the investigation.
- Review events and actions at the conclusion of an incident and make recommendations to the DHS CPO, DHS CIO, and PIRT members (if PIRT is convened) regarding any indicated changes in the DHS technology and incident handling plan.
- Send a copy of any investigation report(s) by email to PIRT members if a PIRT is convened, or if no PIRT is convened, send any report(s) by email to the DHS Deputy Secretary, DHS CPO, DHS CIO, DHS Deputy CIO, DHS OIG, and DHS CISO.
- Upon completion of the investigation, the Component Privacy Office/PPOC will update the Privacy Incident Report at https://soconline@dhs.gov to indicate the closure of the investigation, subject to review by the DHS CPO and DHS CIO. The DHS CPO will consult with DHS senior officials regarding the incident.

8. Notifications and Communications Concerning Privacy Incidents

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

8.1. Internal DHS Notification Procedures

Internal notifications will take two forms: (1) Privacy Incident Notifications automatically generated by the DHS SOC Online Incident Handling System; and (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 SOC Online Incident Handling System

The DHS SOC Online Incident Handling System will automatically send a Privacy Incident Notification at the following stages.

1. After a Component Privacy Officer/PPOC or Component IT Security Entity has opened and completed an incident report, the DHS CPO (Privacy Office) will be notified automatically by DHS SOC. See Diagram E.

2. When the DHS SOC reports the incident to US-CERT, it will also automatically notify the Deputy Secretary, DHS CPO, DHS CIO, DHS Deputy CIO, DHS CISO, and DHS OGC-GLD. See Diagram E.

3. The Component Privacy Office/PPOC and the Component IT Security Entity will update the Privacy Incident Report at https://soconline@dhs.gov to recommend incident closure, subject to review by the DHS CPO and DHS CIO. DHS SOC will automatically issue Privacy Incident Notifications to the DHS Deputy Secretary, DHS CPO, DHS CIO, DHS Deputy CIO, DHS CISO, and DHS OGC-GLD. See Diagram E.

8.1.2. Internal Notification by Email and/or Voicemail

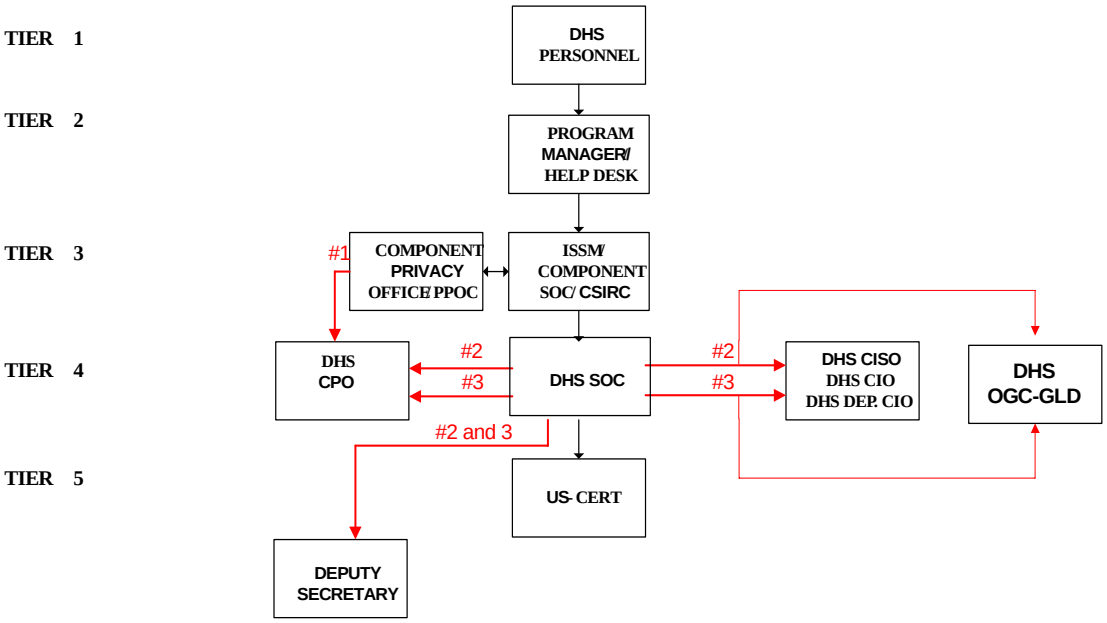


Diagram E: Process Flow for Privacy Incident Notifications Automatically Issued by DHS SOC

Notification must be provided under the following circumstances:

- After the DHS SOC reports the Privacy Incident to US-CERT, a PIRT may be convened for incident handling. The DHS CPO or the Component Privacy Office/PPOC will notify members of the PIRT via a prerecorded voicemail or by email that a Privacy Incident has been reported to US-CERT and that the members of their PIRT are responsible for handling the investigation, notification, if warranted, and mitigation for the Privacy Incident.
- When the DHS SOC has reported an incident solely as a Computer Security Incident and then subsequently determines that the incident in fact involved the potential compromise

of PII, the DHS SOC will notify the DHS Deputy Secretary, DHS CPO, DHS CIO, DHS Deputy CIO, DHS CISO, and DHS OGC-GLD of the change in categorization of the incident.

- If and when it is determined that additional Components (beyond the Component in which the incident occurred) are affected by a Privacy Incident, can notify components directly and document notification in Privacy Incident Report. In addition, the Component Privacy Office/PPOC must notify DHS SOC. Either the Component Privacy Office/PPOC or DHS SOC notifies the DHS Deputy Secretary, DHS CPO, DHS CIO, DHS Deputy CIO, DHS CISO, and DHS OGC-GLD accordingly.
- If the Component Head and the PIRT Chair determine that external notification is warranted, the following will occur:
  - If a D-PIRT has been convened, the Component Head, DHS CPO and the DHS CIO will coordinate with the DHS Public Affairs Office to provide ***reasonable advance internal notice*** to DHS senior officials by email or voicemail of the notification decision ***before external notification*** is made.
  - In all other circumstances, the Component Head will coordinate with the DHS CPO, DHS CIO, the DHS Public Affairs Office and/or the Component communications office to provide ***reasonable advance internal notice*** to DHS senior officials by email or voicemail of the notification decision ***before external notification*** is made.

The Component Privacy Office/PPOC will collect and update POC information concerning C-PIRT members. The Component Privacy Office/PPOC will provide the information to the DHS CPO, DHS CIO, and DHS CISO in a timely manner. DHS CPO collects and maintains POC information from DHS Components and from members of D-PIRT.

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.

DHS personnel must not make or engage in external communications without securing prior authorization from the Component Head and the Chair of the PIRT.

8.2.2. Public Inquires About Privacy Incidents

With respect to all media-related inquiries about Privacy Incidents, the DHS Public Affairs Office will be the sole POC.

For all non-media-related inquiries concerning the status of Privacy Incidents or the implementation of this guidance, the DHS CPO or his/her designee will determine who will handle the inquiry.

8.2.3. Internal Decision-Making Process for External Notification

A decision to publicly release Privacy Incident information will be reached through a collaborative process. Once the Component Privacy Office/PPOC has completed the Escalation Risk Assessment, the Component Head and PIRT (if convened) will promptly review it and enter recommendations and relevant comments, if any, in the External Notification Assessment. See Appendix D for the *External Notification Assessment*. The PIRT will indicate whether it concurs with the notification recommendation contained in the Escalation Risk Assessment using the principles set forth in Section 6.4.6. If notification is warranted, the incident handler (e.g., the Component Privacy Office/PPOC and other PIRT members (if PIRT is convened)) will then proceed to assess the following issues pertaining to 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 the Privacy Incident (Section 8.2.9)

The Component Head and the PIRT Chair will make a joint and final decision as to whether, how, and when external notification will be provided. Before external notification may be provided, internal notification must be given to DHS senior officials. If a D-PIRT has been convened, the DHS CPO and DHS CIO will coordinate with DHS Public Affairs Office to provide *reasonable advance internal notice* to DHS senior officials by email or voicemail of the notification decision before external notification is made. In all other circumstances, the Component Head will coordinate with the DHS CPO, DHS CIO, DHS OGC-GLD, DHS Public Affairs Office and/or the Component communications office to provide *reasonable advance internal notice* to DHS senior officials by email or voicemail of the 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 of this guidance and applies to all external communications, including, but not limited to, congressional notifications, press releases, and notifications of 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 then 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 individual that he/she may designate in writing. In some circumstances, law enforcement or national security considerations may require a delay if it would seriously impede the investigation of the Privacy Incident or the affected individual. However, any delay should not exacerbate risk or harm to any affected individual(s).

8.2.6. Source of Notification

As a general rule, notification to individuals affected by the Privacy Incident should be issued by the DHS Secretary or a senior-level individual that he/she may designate in writing, or, in those instances where the Privacy Incident involves a publicly known Component of DHS, such as the Transportation Security Administration (TSA) or United States Coast Guard, the Component Head.

Notification involving only a limited number of individuals (e.g., under 50) may also be issued jointly by the DHS CPO and DHS CIO.

When the Privacy Incident involves a federal contractor or a public-private partnership operating a system of records on behalf of the agency, 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 should be concise, conspicuous, plain language. The notice should include the following elements:

- Brief description of what happened, including the date(s) of the Privacy Incident and of its 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, disability code, 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 an individual should take to protect themselves from potential harm, if any
- What the agency is doing, if anything, to investigate the Privacy Incident, mitigate losses, and protect against any further Privacy Incidents

- Who affected individuals should contact at the agency for more information, including a toll-free telephone number, email address, and postal address.

A copy of a sample notification letter is attached to this guidance as Appendix F.

8.2.7.2. Translation of Notice into Other Languages

Effective Privacy Incident handling necessitates that individuals affected by the Privacy Incident must understand the importance of the notification. Therefore, if the Component's record states 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 upon 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 personalized notification and/or when a limited number of individuals are affected. Telephone notification, however, should be associated with written notification by first-class mail.

8.2.8.2. First-Class Mail

First-class mail notification to the last known mailing address of the individual in the DHS records should be the primary means notification is provided. Where 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 notice should be sent separately from any other mailing so that it is conspicuous to the recipient. If the agency that experienced the Privacy Incident uses another agency to facilitate mailing (for example, if the agency that suffered the loss consults with the Internal Revenue Service [IRS]for current mailing addresses of affected individuals) care should be taken to ensure that the agency that suffered the loss is identified as the sender, and not the facilitating agency. The front of the envelope should be labeled to alert the recipient to the importance of its contents (e.g., "Data Breach Information Enclosed") and should be marked with the name of your agency as the sender to reduce the likelihood that the recipient thinks it is advertising mail.

8.2.8.3. Email

Email notification is problematic because individuals change their email addresses and often do not notify third parties of the change. Notification by postal mail is preferable. However, where 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 also be employed in conjunction with postal mail if the circumstances of the Privacy Incident warrant this approach. Email notification may include links to the agency 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. *See Appendix G for a Sample Press Release.* The affected Component may set up toll-free call centers staffed by trained personnel to handle inquiries from the affected individuals and the public.

8.2.8.6. Substitute Notice

Substitute notice may be appropriate in those instances where DHS does not have sufficient contact information to provide notification. Substitute notice should consist of a conspicuous posting of the notice in two ways:

- On the home page of the DHS web site or on the home page of the affected Component's web site if the Component is a publicly known Component such as TSA or the Federal Emergency Management Agency (FEMA); and
- Notification to major print and broadcast media, including major media in areas where the affected individuals reside.

The notice to media should include a toll-free phone 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 providing notice 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 or posting a large type notice on the DHS and Component web sites.

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 for law enforcement or national security reasons, all affected individuals should receive prompt notification. See Appendix F for a copy of a sample notification letter. In the end, if the five factors set forth in Section 6.3 of this guidance are applied appropriately within the fact-specific context, notification will only be given when there is a reasonable risk of harm and when it will not lead to the overuse of notification.

8.2.9.2. Notification of Third Parties including the Media

The 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 that it does not unnecessarily alarm the public. When appropriate, public media should be notified as soon as possible after the discovery of a breach and the incident 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 upon 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. See Appendix G for a copy of a sample press release.

8.2.9.2.2. Web Posting

DHS should post information about the Privacy Incident and notification in a clearly identifiable location on the home pages of the DHS web site and the Component's web site 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 (FAQ) and other talking points to assist the public's understanding of the Privacy Incident and the notification process. The information should also appear on the www.Firstgov.gov web site. The affected Component may also consult with General Services Administration (GSA) USA Services regarding using their call center. See the FAQ posted by the Department of Veterans Affairs (VA) in response to the May 2006 incident at www.firstgov.gov/veteransinfo.shtml for examples of links to identity theft resources and a sample FAQ.

8.2.9.2.3. Notification of other Public and Private Sector Agencies

The Component Head and Component Privacy Office/PPOC for the affected Component will work in close consultation with the DHS CPO and DHS CIO in evaluating whether other public and private sector agencies may need to be notified on a need to know basis, particularly those which 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 organizations and individuals understand that any further unnecessary disclosure of the personal data of individuals affected by the Privacy Incident would only exacerbate an already stressful and potentially costly problem for the individuals involved. Therefore, the disclosure of PII, particularly sensitive PII, must be circumscribed and carefully deliberated.

8.2.9.2.4. Congressional Inquiries

DHS should be prepared to respond to inquires from other governmental agencies such as the Government Accountability Office (GAO) and Congress. The Component Head, Chair of the PIRT (if a PIRT is convened), DHS CPO, DHS CIO and DHS Legislative Affairs Office will work in close consultation to determine when notification of the incident should be provided to the congressional oversight committee chairs. With respect to a High-Impact Privacy Incidents, the DHS Legislative Affairs Office and DHS Public Affairs Office will coordinate so that notification to the appropriate committee Chair is issued in advance of or simultaneously 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. See FIPS Pub 199, February 2004; http://csrc.nist.gov/publications/fips/. The impact levels – low, moderate, and high, describe the (worst case) potential impact on an organization or individual if a breach of security occurs. The determination of the potential impact of loss of information is made by DHS during an information system's C&A process.

- **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 6.3 of the PIHG 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 SOC 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)) should be attached to the Privacy Incident Report in the DHS SOC Online Incident Handling System.

9. Mitigation

9.1. Purpose of Mitigation: Containment of Source and Prevention or Minimization of Consequent 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 simultaneously consider options for reducing that risk. The Component Privacy Office, PPOC, PIRT, Component IT Security Entity, and PM will have a central role in implementing countermeasures to mitigate the potential harm posed by the Privacy Incident. *See Appendix C for the DHS Privacy Playbook: Handling Process Overview* for an overview and checklist for the incident mitigation process. Mitigation is an essential aspect of the agency's effort to contain the source of a Privacy Incident and to identify and to lessen the potential harm that the loss, compromise, or misuse of the PII may have on affected individuals.

9.2. Timing and Sequence of Mitigation

Mitigation is not a 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 warranted by the circumstances of the incident.

9.3. Harm Defined

Harm is defined as follows:

> 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 on 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; 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.

9.4. Division of Mitigation Responsibilities

The Component Privacy Office/PPOC will work in consultation with the Component IT Security Entity, PIRT (if convened), and PM to prevent or minimize any consequent harm. The first step of the mitigation process may be performed by the PMs, particularly in gathering, securing, and documenting evidence of the incident. Therefore, PMs will collaborate with the Component Privacy Office/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 the IT security issues pertaining to the incident and will implement containment measures for IT systems in accordance with the CONOPS and DHS Sensitive Systems Directive 4300A. Their responsibilities include:

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

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

The Component Privacy Office/PPOC will address the privacy ramifications of a Privacy Incident and will focus on preventing or minimizing any consequent harm to affected individuals. As such, mitigation will involve activity beyond the securing of a system (electronic or paper) and isolating the vulnerability. The Component Privacy Office/PPOC should consider a broad range of countermeasures as dictated by the nature and sensitivity of the PII. An effective response may necessitate 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, but is not limited to:

- Notification of 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 Office/PPOC in coordination with Component SOC or DHS SOC Security Technical Support 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 is suspected, the Component Privacy Office/PPOC in coordination with Component SOC or DHS SOC Security Technical Support Officer will ensure consultation and reporting with the Component CSO; Component CSO will determines whether to contact law enforcement (internal or external).
- Notification and involvement of external law enforcement must be documented in the Privacy Incident Report.
- Contacting the issuing bank for incidents involving credit cards pursuant to Sections 5 and 6 of this guidance
- Offering credit monitoring services to mitigate the misuse of the PII and identify patterns of suspicious behavior

9.5. Mitigation Countermeasures Must be Documented

All mitigation measures implemented must be documented in the Privacy Incident Report or in the Escalation Risk Assessment in the DHS SOC Online Incident Handling System.

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

10.1. Overview

DHS personnel, including employees, supervisors, managers, and contractors, have privacy and security responsibilities to safeguard PII imposed by federal laws, regulations, and directives, and Departmental directives and guidance. *See listing of authorities in Section 2.3.*

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 as follows:

- *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).

10.2. 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.

A Privacy Threshold Analysis (PTA) must be performed for all IT systems to determine whether or not a full PIA is required. The purpose of a PIA is to demonstrate that system owners and developers have consciously incorporated privacy protections throughout the lifecycle of a system.

OMB M-06-16 (*Protection of Sensitive Agency Information*) requires that agencies protect PII that is physically removed from the agency location or that is accessed remotely. Physical removal includes both removable media as well as media within mobile devices (e.g., laptop hard drive).

General policies relating to PII are provided below. Additional PII-related policies are included in the following sections of the DHS 4300A Sensitive Systems Handbook:

- Section 3.9: C&A. For systems involving PII, the confidentiality security objective shall be assigned an impact level of at least moderate.
- Section 4.8.2: Laptop Computers and Other Mobile Computing Devices. All information stored on any laptop computer or other mobile computing device is to be encrypted.
- Section 5.2.2: Automatic Session Lockout. Sessions on workstations and on laptop computers and other mobile computing devices are to be terminated after 20 minutes of inactivity.
- Section 5.3: Auditing. Policies on audit logs of computer-readable extracts of PII from databases and on erasure of these extracts are provided.
- Section 5.4.1: Remote Access and Dial-in. Remote access of PII must be approved by the Designated Accrediting Authority (DAA). Strong authentication via virtual private network (VPN) or equivalent encryption (e.g., https) and two-factor authentication is required. Restrictions are placed on the downloading and remote storage of PII accessed remotely.

DHS Policy
a. PII shall not be physically removed from a DHS facility without written authorization from the system DAA or person designated in writing by the DAA.
b. PII removed from a DHS facility shall be encrypted.
c. If PII can be physically removed from an IT system (printouts, CDs, etc), the System Security Plan shall document the specific procedures, training, and accountability measures in place to ensure that remote use of the encrypted data does not bypass the protections provided by the encryption.

10.3. Basis for Disciplinary or Corrective Action

Disciplinary or corrective action regarding DHS personnel (including employees, supervisors, and managers) may be based upon 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, failure to adequately instruct, train, or supervise employees in their responsibilities; and
- For 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.

10.4. Consequences

Applicable consequences may include reprimand, suspension, removal, or other actions in accordance with applicable law and agency policy. At a minimum, the 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* 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

DHS Policy
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.

10.5. Procedure

The Component Privacy Office/PPOC must inform the head of the Component where DHS personnel has failed to implement safeguards to protect PII or where 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. See DHS Sensitive Systems 4300A; see also Appendix C for the *DHS Privacy Playbook: Handling Process Overview* for an overview and checklist for the process for pursuing 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 commensurate with 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 the DHS OIG, DHS OGC-GLD and CHCO in the event that the Privacy Incident arises from violations or potential violations of the ethics statutes or regulations.

The Component Privacy Office/PPOC must also notify the DHS OGC-GLD and Component OGC-GLD where DHS personnel (including employees, supervisors, and managers) fail to implement safeguards to protect PII or where 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-GLD or Component OGC-GLD will consult with the Component Privacy Office/PPOC or other PIRT members, the Component Head, and CHCO on legal issues pertaining to disciplinary or corrective action.

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

The Component Privacy Office/PPOC must 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 will provide a thorough explanation of the following:

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

- The 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 external law enforcement, that fact should be reported.

Any DHS personnel who is the subject of 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 notation of the fact 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 action taken against DHS personnel that arise out of a Privacy Incident.

11. Closure of Privacy Incidents

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

The Component Privacy Office/PPOC will update the Privacy Incident Report https://soconline@dhs.gov to recommend incident closure, subject to review by the DHS CPO and DHS CIO. DHS CSIRC/SOC will make the closure recommendation in weekly status reports of ongoing Privacy Incidents. The Privacy Incident Report is closed unless the DHS CPO or DHS CIO notifies the DHS SOC that the incident must remain open for review or further incident handling. The DHS SOC will issue closure notifications to the DHS Deputy Secretary, DHS CPO, DHS CIO, DHS Deputy CIO, DHS CISO, and DHS OGC-GLD monthly.

12. Annual Program Review of the Implementation of the PIHG

Members of the D-PIRT and other DHS senior officials as designated are responsible for conducting an annual review of the implementation of the PIHG at the Departmental and Component levels. *See Appendix C for the DHS Privacy Playbook: Handling Process Overview* for an overview and checklist for the incident handling process. The review process will include the following:

- 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 must be revised in order to strengthen DHS safeguards for PII;
- Identification and adoption of best practices that must be incorporated in the PIHG; and
- Examination of training programs pertaining to the implementation of the PIHG and the safeguarding of PII.

The DHS CPO will chair the review process and will prepare the Annual Report for the Program Review of the PIHG.

13. 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 C 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 will continue to implement training programs that address:

- The rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of the [Privacy Act], including any other rules and procedures adopted pursuant to [the Privacy Act] and the penalties for noncompliance." (5 U.S.C. § 522a(e)(9))
- The "administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained." (5 U.S.C. § 552a(e)(10)

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 will provide at least annual refresher training to ensure that employees continue to understand their responsibilities**.** Such programs will 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 sign at least annually a document clearly describing their responsibilities.

Privacy Incident Handling Guidance

Appendices

September 10, 2007

Basis for Privacy Incident Handling Guidance

These Appendices supports the Department of Homeland Security (DHS) Privacy Incident Handling Guidance (PIHG).

TABLE OF CONTENTS

Appendix A: Illustrations of Privacy Incidents

Definition of Privacy Incident

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 and for an other than authorized purpose have access or potential access to personally identifiable information in usable form, whether physical or electronic." (See Office of Management and Budget (OMB) Memorandum 07-16 [M-07-16], at 2 and 9). The term encompasses both **suspected and confirmed incidents** involving personally identifiable information (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 OMB M-07-16, at 1 n.5).

Definition of Personally Identifiable Information

Personally Identifiable Information 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.

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, Official Guidance*, Department of Homeland Security (DHS) Privacy Office.

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: social security number, driver's license 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. In addition, the context of the PII may determine whether the PII 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 PII on 120 component employees who have recently separated from or retired from federal service. These paper records have ***full names, dates of birth, SSNs, and financial information (including salary and bank information)***.
- Lost thumb drive: An employee reports a lost 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.
- An employee reports that a paper file is missing from her desk. The file contains a printout with the ***last four digits of the government travel cards*** belonging to employees within the reporting employee's division.
- A system containing research data where the ***data has been scrubbed to de-personalize individuals*** was compromised by a hacker who cracked a password or user account and installed hacking software. No PII was compromised, but the intruder had read/write access to the server and was able to open access points

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 DHS Online intranet.
- An employee disposed of boxes containing sensitive information in a trash dumpster; the box 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 and fingerprints***.

- Documents containing the ***name, weight, height, eye and hair color*** of several new employees were mistakenly faxed from one agency's security office to a government agency that was not authorized to receive the information. The originating agency's security officer does not believe that the information was compromised because the unauthorized recipient promptly destroyed the information upon receipt.

Unauthorized Acquisition

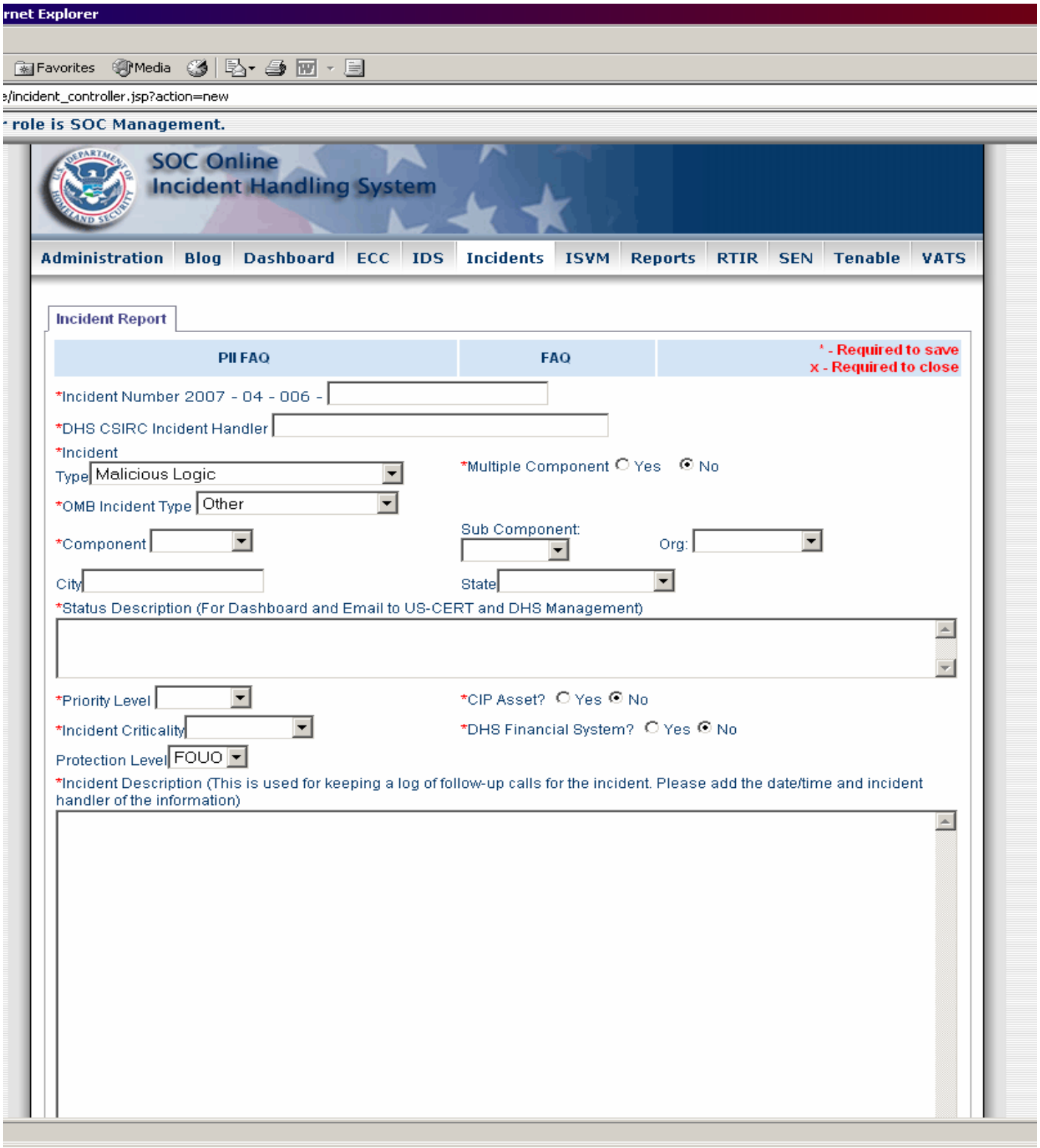
- An employee reports that he had inadvertently acquired access to five other federal employees' ***government credit card numbers and Personal Identification Numbers*** (PIN) located on the travel vouchers in the agency's Travel Management System.
- An employee finds a box of documents outside of a 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 agency and/or customer computer systems, allowing the ***capture of passwords, IP addresses, and URLs of websites*** visited by the employees and customers by an unknown source.

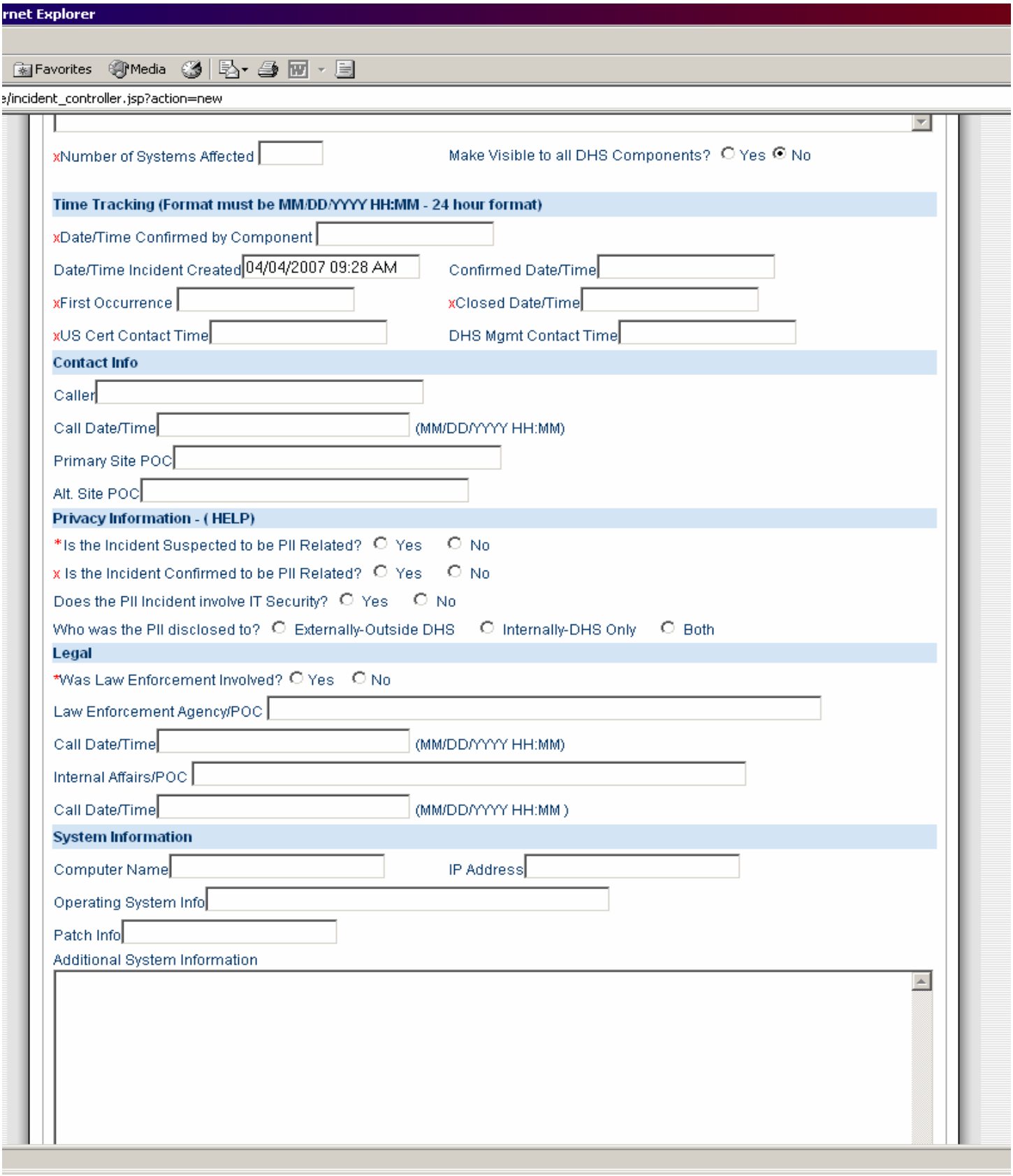
Unauthorized Access (Internal and External)

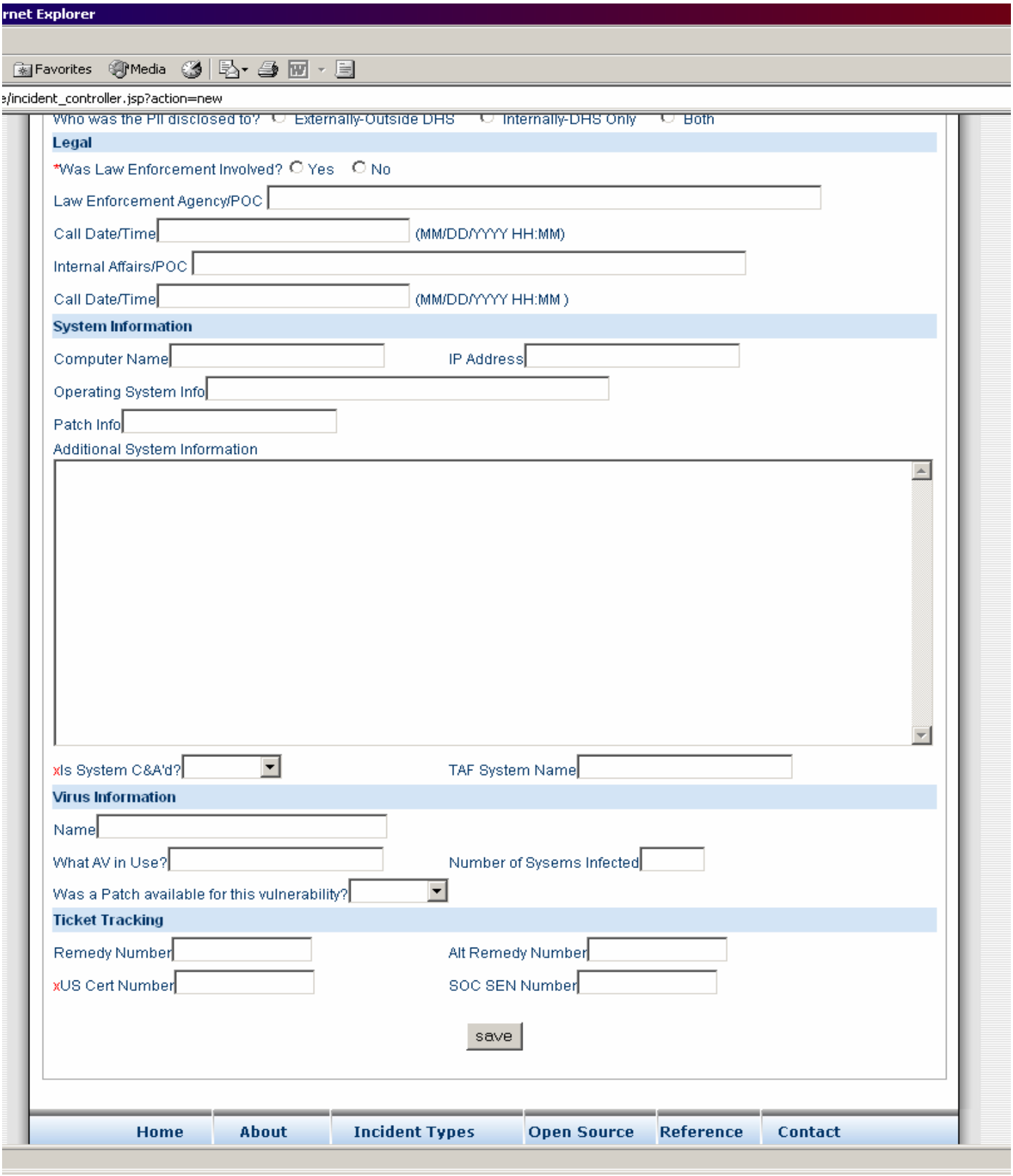
- A contractor who misused administrator privileges gained unauthorized access to a procurement system and posted sensitive information on ***contract bids, government procurement card numbers, and tax identification numbers*** on the agency's Internet web site, exposing an unknown amount of PII.
- An unknown person gained unauthorized access to a component field office. This intruder implanted malicious software in the system that caused the transfer of files containing ***names, home addresses, salaries, and bank account numbers*** of 1700 individuals.
- A glitch on the component's Internet web page allows unauthorized read-only access to a database containing benefits information on 3,000 individuals.

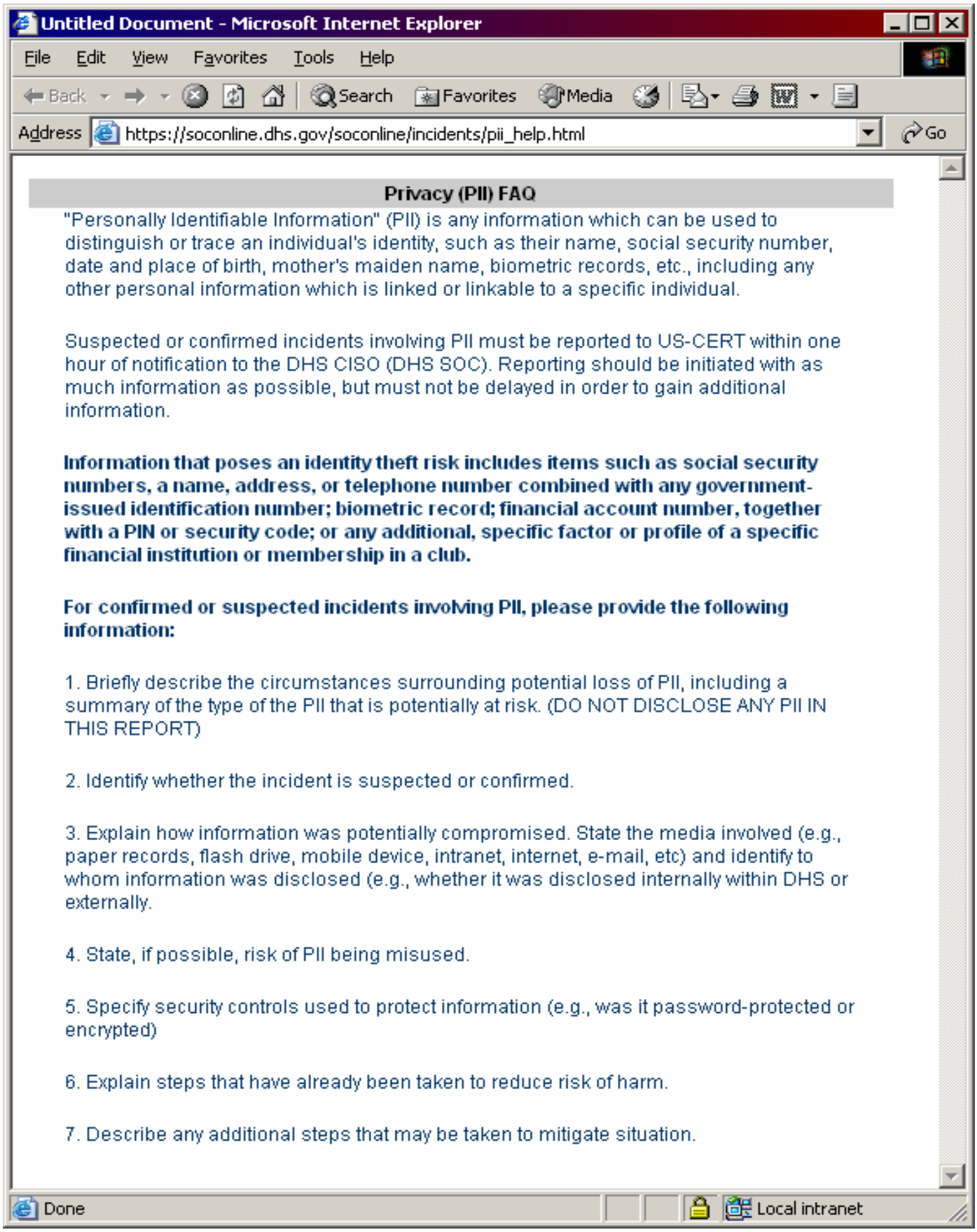
  Only the ***unique case number*** of each individual is viewable and this unique identifier cannot be used to access any information of beneficiaries, such as name, address, zip code, SSN, telephone number, and date of birth.

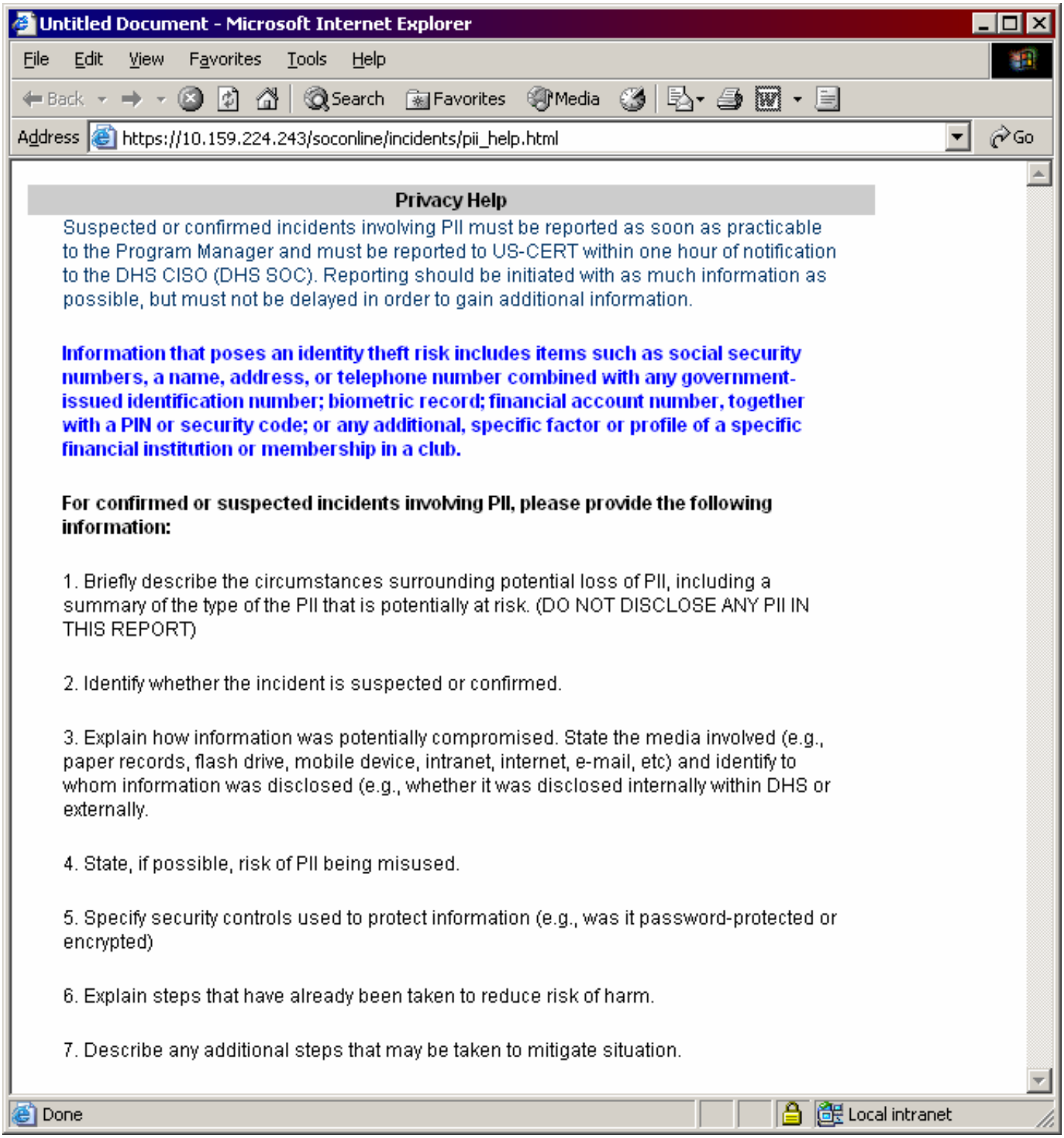
Appendix B: Privacy Incident Report Template




rnet Explorer
Favorites
Media
e/incident_controller.jsp?action=new
xNumber of Systems Affected
Make Visible to all DHS Components? Yes No
Time Tracking (Format must be MM/DD/YYYY HH:MM - 24 hour format)
xDate/Time Confirmed by Component
Date/Time Incident Created 04/04/2007 09:28 AM
Confirmed Date/Time
xFirst Occurrence
xClosed Date/Time
xUS Cert Contact Time
DHS Mgmt Contact Time
Contact Info
Caller
Call Date/Time (MM/DD/YYYY HH:MM)
Primary Site POC
Alt. Site POC
Privacy Information - (HELP)
*Is the Incident Suspected to be PII Related? Yes No
x Is the Incident Confirmed to be PII Related? Yes No
Does the PII Incident involve IT Security? Yes No
Who was the PII disclosed to? Externally-Outside DHS Internally-DHS Only Both
Legal
*Was Law Enforcement Involved? Yes No
Law Enforcement Agency/POC
Call Date/Time (MM/DD/YYYY HH:MM)
Internal Affairs/POC
Call Date/Time (MM/DD/YYYY HH:MM)
System Information
Computer Name
IP Address
Operating System Info
Patch Info
Additional System Information


rnet Explorer
Favorites
Media
e/incident_controller.jsp?action=new
Who was the PII disclosed to? Externally-Outside DHS Internally-DHS Only Both
Legal
*Was Law Enforcement Involved? Yes No
Law Enforcement Agency/POC
Call Date/Time (MM/DD/YYYY HH:MM)
Internal Affairs/POC
Call Date/Time (MM/DD/YYYY HH:MM)
System Information
Computer Name
IP Address
Operating System Info
Patch Info
Additional System Information
xIs System C&A'd?
TAF System Name
Virus Information
Name
What AV in Use?
Number of Sysems Infected
Was a Patch available for this vulnerability?
Ticket Tracking
Remedy Number
Alt Remedy Number
xUS Cert Number
SOC SEN Number
save
Home
About
Incident Types
Open Source
Reference
Contact


Untitled Document - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://soconline.dhs.gov/soconline/incidents/pii_help.html
Go
Privacy (PII) FAQ
"Personally Identifiable Information" (PII) is any information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to a specific individual.
Suspected or confirmed incidents involving PII must be reported to US-CERT within one hour of notification to the DHS CISO (DHS SOC). Reporting should be initiated with as much information as possible, but must not be delayed in order to gain additional information.
Information that poses an identity theft risk includes items such as social security numbers, a name, address, or telephone number combined with any government-issued identification number; biometric record; financial account number, together with a PIN or security code; or any additional, specific factor or profile of a specific financial institution or membership in a club.
For confirmed or suspected incidents involving PII, please provide the following information:
1. Briefly describe the circumstances surrounding potential loss of PII, including a summary of the type of the PII that is potentially at risk. (DO NOT DISCLOSE ANY PII IN THIS REPORT)
2. Identify whether the incident is suspected or confirmed.
3. Explain how information was potentially compromised. State the media involved (e.g., paper records, flash drive, mobile device, intranet, internet, e-mail, etc) and identify to whom information was disclosed (e.g., whether it was disclosed internally within DHS or externally.
4. State, if possible, risk of PII being misused.
5. Specify security controls used to protect information (e.g., was it password-protected or encrypted)
6. Explain steps that have already been taken to reduce risk of harm.
7. Describe any additional steps that may be taken to mitigate situation.
Done
Local intranet


Untitled Document - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://10.159.224.243/soconline/incidents/pii_help.html
Go
Privacy Help
Suspected or confirmed incidents involving PII must be reported as soon as practicable to the Program Manager and must be reported to US-CERT within one hour of notification to the DHS CISO (DHS SOC). Reporting should be initiated with as much information as possible, but must not be delayed in order to gain additional information.
Information that poses an identity theft risk includes items such as social security numbers, a name, address, or telephone number combined with any government-issued identification number; biometric record; financial account number, together with a PIN or security code; or any additional, specific factor or profile of a specific financial institution or membership in a club.
For confirmed or suspected incidents involving PII, please provide the following information:
1. Briefly describe the circumstances surrounding potential loss of PII, including a summary of the type of the PII that is potentially at risk. (DO NOT DISCLOSE ANY PII IN THIS REPORT)
2. Identify whether the incident is suspected or confirmed.
3. Explain how information was potentially compromised. State the media involved (e.g., paper records, flash drive, mobile device, intranet, internet, e-mail, etc) and identify to whom information was disclosed (e.g., whether it was disclosed internally within DHS or externally.
4. State, if possible, risk of PII being misused.
5. Specify security controls used to protect information (e.g., was it password-protected or encrypted)
6. Explain steps that have already been taken to reduce risk of harm.
7. Describe any additional steps that may be taken to mitigate situation.
Done
Local intranet

Appendix C: 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 1 hour of notice to the DHS Chief Information Security Officer (CISO).**

DHS personnel must expedite reporting to ensure compliance with the mandatory OMB 1-hour requirement. The incident handler must prioritize the activities identified in the following Process Overview as circumstances warrant. For a graphic display of the incident handling process, refer to Appendix E.

Handling Process Overview

Reporting (Section 5)		
	DHS personnel detects incident that may involve PII.	
	DHS personnel notifies Program Manager (PM) of suspected or confirmed incident. If PM is not available, DHS personnel contacts 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., 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 Office/Privacy Office Point of Contact (PPOC) to confirm whether Privacy Incident has occurred and to coordinate incident handling.	
	Component Privacy Office/PPOC or Component IT Security Entity enters report data into DHS SOC Online Incident Handling System at https://soconline.dhs.gov.	
	DHS SOC/CSIRC automatically sends Privacy Incident Notification regarding entry of report in DHS SOC Online Handling System to DHS CPO at DHSPrivacyIncident@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 Chief Information Officer (CIO), DHS Deputy CIO, DHS CISO, and DHS Office of General Counsel, General Law Division (OGC-GLD) alerting DHS senior officials of report to US-CERT.	
	Component Privacy Office/PPOC notifies DHS Chief Financial Officer (CFO) of any Privacy Incident involving government-authorized credit cards.	
		DHS CFO notifies the issuing bank(s) of the incident where appropriate.
		The Component Privacy Office/PPOC supplements the Privacy Incident Report to reflect the CFO's notification of the issuing bank(s) (where appropriate).
	Component Privacy Office/PPOC notifies the DHS CFO of any Privacy Incident involving individuals' bank account numbers to be used for the direct deposit of credit card reimbursements, government employee salaries, or any benefit information.	
		The DHS CFO notifies the Chief Human Capital Officer (CHCO) and the issuing bank(s) of the incident (where appropriate).
		DHS CFO informs the Component Privacy Office/PPOC of such notification.
		Component Privacy Office/PPOC supplements the Privacy Incident Report to reflect the CFO's notification of issuing bank(s).
	Component ISSMs and the Component Privacy Office/PPOC report Privacy Incidents involving CFO	

	Designated Financial Systems to the Component CFO.
	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 Office/PPOC notifies the DHS SOC. DHS SOC then notifies: the DHS Deputy Secretary, DHS CPO, DHS CIO, DHS Deputy CIO, DHS CISO, and DHS OGC-GLD of the change in categorization. □ If a Privacy Incident impacts the security of an IT system, the PM refer to the DHS SOC CONOPS document for incident handling requirements.
	If the Component Privacy Office/PPOC determines that the incident affects additional components (beyond the Component in which the incident occurred), the Component Privacy Office/PPOC can notify components directly and document notification in Privacy Incident Report. In addition, the Component Privacy Office/PPOC must notify DHS SOC. Either the Component Privacy Office/PPOC or DHS SOC notifies: the DHS Deputy Secretary, DHS CPO, DHS CIO, DHS Deputy CIO, DHS CISO, and DHS OGC-GLD of the subsequent change of substantive facts.
	DHS CIO notifies the DHS Chief Security Office (CSO) when the incident involves security-related issues affected DHS personnel, property, facilities, and information.
	US-CERT reports the incident to the appropriate external government entities.
	Component Privacy Office/PPOC responds to inquiries from US-CERT regarding the Privacy Incident.
	Component Privacy Office/PPOC supplements report at https://soconline.dhs.gov as needed.
Escalation to Determine Who Handles Incident and To Make Preliminary Recommendation Regarding Notification (Section 6)	
	Component Privacy Office/PPOC conducts a risk analysis of the incident and documents the analysis in the Escalation Risk Assessment in the DHS SOC Online Incident Handling System.
	Component Privacy Office/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 Office/PPOC immediately evaluates the context of the incident and the PII that was potentially or actually lost or compromised.
	Component Privacy Office/PPOC identifies the type of risk involved in the incident.
	The Component Privacy Office/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 together with a PIN or security code (if a PIN or security code is necessary to access the account); 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, driver's license number; financial account number; citizenship or immigration status; or medical information. □ If the Component Privacy Office/PPOC neither suspects nor confirms that identity theft is implicated, then the Component Privacy Office/PPOC proceeds with the evaluation of the five factors determining the likely risk of harm. □ If identity theft is implicated, the Component Privacy Office/PPOC immediately notifies the DHS Office of the Inspector General (OIG) and DHS Privacy Office. Together, in close consultation, they analyze and complete the Escalation Risk Assessment.

Component Privacy Office/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;
  - ☐ Where criminal activity is suspected or confirmed, the Component Privacy Office/PPOC promptly notifies DHS SOC and DHS CSO.
    - Component Privacy Office/PPOC, in coordination with Component SOC or DHS SOC Security Technical Support 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, DHS OIG, and DHS OGC-GLD.
    - If criminal activity impacts physical security, the Component Privacy Office/PPOC, in coordination with Component SOC or DHS SOC Security Technical Support Officer, will ensure consultation and reporting with the Component CSO; Component CSO will determines whether to contact law enforcement (internal or external).
- ☐ The ability to mitigate the risk of harm.

Component Privacy Office/PPOC assigns an impact level of low, moderate, or high to each risk factor.

If incident involves a risk of identity theft, the categorization is performed in consultation with DHS OIG and the DHS Privacy Office.

The likely risk of harm is LOW where 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 Encryption and validated by the National Institute of Standards and Technology [NIST]).

The likely risk of harm is MODERATE or HIGH where criminal activity is suspected or confirmed.

- Component Privacy Office/PPOC, in coordination with Component SOC or DHS SOC Security Technical Support 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, DHS OIG, and DHS OGC-GLD.
- If criminal activity impacts physical security, the Component Privacy Office/PPOC, in coordination with Component SOC or DHS SOC Security Technical Support Officer, will ensure consultation and reporting with the Component CSO; Component CSO will determines whether to contact law enforcement (internal or external)..
- Notification and involvement of external law enforcement must be documented in the Privacy Incident Report.

All Sensitive PII must be designated as MODERATE or HIGH impact.

Component Privacy Office/PPOC recommends who should handle the incident (e.g., Component Privacy Office/PPOC, Component-level Privacy Incident Response Team [C-PIRT], or Departmental-level Privacy Incident Response Team [D-PIRT]) for purposes of investigation, notification, mitigation, and closure.

If Component Privacy Office/PPOC determines that the incident creates a minimal risk of harm, the incident has a low impact and Component Privacy Office/PPOC will not escalate incident to CPO for investigation, mitigation, notification, and closure; Component Privacy Office/PPOC will handle incident with guidance, as needed, from the DHS Privacy Office.

		If the incident meets or exceeds the reasonable risk of harm standard, its potential impact is Moderate or High. The following guidelines apply: The likely risk of harm is MODERATE or HIGH where criminal activity is suspected or confirmed. If the potential impact is Moderate, the Component Privacy Office/PPOC may convene a C-PIRT • If C-PIRT is convened, Component Privacy Office/PPOC: ▪ Serves as the Chair of C-PIRT; and ▪ Promptly notifies the C-PIRT members of the Privacy Incident • If C-PIRT is not convened, the Component Privacy Office/PPOC handles the incident with guidance as needed from the DHS Privacy Office. DHS Privacy Office and DHS senior officials follow the best judgment standard in deciding whether D-PIRT handles the response for the incident. A D-PIRT may be convened where: ☐ The *potential impact* of the Privacy Incident is HIGH; or ☐ The *potential impact* of the Privacy Incident is MODERATE but occurred at DHS Headquarters; the DHS Privacy Office performs the functions of the Component Privacy Office/PPOC with respect to incident handling. A D-PIRT may be convened by the DHS Secretary or DHS Deputy Secretary (at their discretion) or other DHS senior officials, as warranted by the circumstances, such as the DHS CPO, DHS CIO, or DHS CISO.. DHS senior officials decide who serves as the D-PIRT Chair for the incident. D-PIRT Chair notifies members that a Privacy Incident has been reported to US-CERT and informs them that they will handle the Privacy Incident.
		The Component Privacy Office/PPOC sends the Escalation Risk Assessment to PIRT members via email.
	If the incident involves government-authorized credit cards, individuals' bank account numbers to be used for the direct deposit of credit card reimbursements, government employee salaries, or any benefit information, or CFO Designated Financial Systems, the Component Privacy Office/PPOC consults with the DHS CFO to determine whether the DHS CFO or the Component CFO should be designated as a PIRT member (if a PIRT is convened).	
	DHS CIO notifies DHS CSO where the incident involves security-related issues affecting DHS personnel, property, facilities, and information.	
	Component Privacy Office/PPOC makes a preliminary recommendation as to whether notification is warranted; if incident involves a risk of identity theft, the decision is made in consultation with DHS OIG and the DHS Privacy Office.	
		Component Privacy Office/PPOC recommends notification where 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 is applicable to restore the reasonable integrity of the data system.
	Component Privacy Office/PPOC identifies the steps DHS should take to mitigate the risk of harm; if incident involves a risk of identity theft, Component Privacy Office/PPOC consults with the DHS OIG and DHS Privacy Office to identify a mitigation plan.	
	The Component Privacy Office/PPOC attaches Escalation Risk Assessment to the Privacy Incident Report and sends the report via email to the DHS Deputy Secretary, DHS Privacy Office at DHSPrivacyIncident@dhs.gov, DHS CIO, and DHS CISO.	
Investigation [PIRT members, Component Privacy Office/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 happened as follows:

- ☐ Document the investigation and gather all information necessary to describe and address the incident.
- ☐ Review the Privacy Incident Report submitted to US-CERT and identify any additional information necessary.
- ☐ Confirm what personal information is lost or at risk.
- ☐ Identify the steps taken to reduce the risk of harm.

Investigators develop a plan of action.

If a PIRT is convened, PIRT clearly delineates investigative responsibilities of each PIRT member based upon the capability, expertise, and authority of each PIRT member in order to ensure proper handling of the Privacy Incident and to avoid duplicative efforts.

The lead investigator must be identified for a particular Privacy Incident. It should be someone who is trained in or familiar with incident response procedures and the complexities involved with the potential loss or compromise of PII:

- If no 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, however, the lead investigator must also report to the DHS OIG and DHS OGC-GLD.
- If a D-PIRT is convened, depending upon the circumstances, the lead investigator will report to the Chair of the D-PIRT or his/her designee.
- If a C-PIRT is convened, depending upon the circumstances, the lead investigator may report to the Chair of the C-PIRT or his/her designee.
- The lead investigator should consult with Component Office of the Chief Counsel or DHS OGC-GLD before initiating investigation on issues pertaining to the handling of evidence and chain of custody.

Investigators follow the DHS internal incident handling procedures:

- Identify what further steps must be taken for the formulation of any further response by DHS.
- Analyze the precedents and indications regarding computer security.
- 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 Office of the Chief Counsel or DHS OGC-DHS to address issues pertaining to 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 all personnel who have 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.

External notification to law enforcement, where criminal activity is suspected or confirmed, should be handled by Component CSO and/or DHS CSO depending on level and severity of criminal activity. The Component Privacy Office/PPOC will coordinate with Component SOC or DHS SOC Security Technical Support Officer, in consultation with the DHS CPO. Notification and involvement of 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 then consults with the lead investigator and other PIRT members as warranted. In incidents in which criminal activity is suspected or confirmed, the lead investigator consults with law enforcement, the DHS OIG, and the Component CSO regarding the closure of the investigation.

	Investigators review events and actions at the conclusion of an incident and make recommendations to the DHS CPO, DHS CIO and PIRT members (if convened) regarding any indicated changes in the DHS technology and incident handling plan.
	Lead investigator sends a copy of any investigation report(s) by email to PIRT members if a PIRT is convened. If no PIRT is convened, the Component Privacy Office/PPOC or Component IT Security Entity sends any report(s) by email to the DHS Deputy Secretary, DHS CPO, DHS CIO, DHS Deputy CIO, and DHS CISO.
	Upon completion of the investigation, the Component Privacy Office/PPOC updates the Privacy Incident Report at https://soconline@dhs.gov to indicate the closure of the investigation, subject to review by the DHS CPO and DHS CIO. DHS CPO consults with DHS senior officials regarding closure of the investigation, as needed.
Notification (Section 8)	
	Component Head and PIRT (if convened) review the recommendations of the Component Privacy Office/PPOC contained in the Escalation Risk Assessment, assess the likely risk of harm posed by the incident, and enter their recommendations regarding external notification in the External Notification Assessment.
	If the Component Head and PIRT preliminarily conclude that notification should be provided, the Component Privacy Office/PPOC and other PIRT members (if convened) then assess when and how external notification should be given (e.g., timing of notification, source of notification, means for providing notification, and who should receive notification).
	PIRT members review the Federal Information Processing Standard (FIPS) Publication (Pub) 199 classification of the information to determine whether the previously assessed level of potential (worst case) impact due to the loss or compromise of PII should be reassessed. Greater weight is given to the likelihood that the information is accessible and usable and whether the Privacy Incident may lead to harm. Notification is provided only where there is a reasonable risk of harm and where notification regarding that particular incident will not lead to overuse of notification.
	PIRT members consult with each other and make a recommendation to the Component Head regarding external notification.
	The Component Head and the PIRT Chair make a joint and final decision as to whether, how and when external notification will be provided.
	If the Component Head and the PIRT Chair determine that external notification is warranted, the following occurs: ☐ Component Privacy Office/PPOC prepares a proposed draft notification letter (without any PII concerning the affected individuals included in the draft) and proposed draft/press release (if any) for consideration by the Component Head. ☐ If a D-PIRT has been convened, the Component Head, DHS CPO, and DHS CIO coordinate with the DHS Public Affairs Office to provide ***reasonable advance internal notice*** to DHS senior officials by email or voicemail of the notification decision ***before external notification*** is made. ☐ In all other circumstances, the Component Head coordinates with the DHS CPO, DHS CIO, the DHS Public Affairs Office and/or the Component communications office to provide ***reasonable advance internal notice*** to DHS senior officials by email or voicemail of the notification decision ***before external notification*** is made. ☐ The Component Head, PIRT Chair (if convened), DHS CPO, DHS CIO, and DHS Legislative Affairs Office coordinate to determine whether notification of the incident should be provided to the congressional oversight committee chairs. ☐ If the incident is categorized as a High-Impact Privacy Incident, the DHS Legislative Affairs Office and DHS Public Affairs Office coordinate notification to the appropriate committee chair(s), which is issued in advance of or simultaneously with the issuance of a press release or notification to affected individuals.
	Component Privacy Office/PPOC sends notification letter to affected third parties.
	Component Privacy Office/PPOC attaches notification documents to the Privacy Incident Report in the DHS SOC Online Incident Handling System (e.g., External Notification Assessment, press release, notification letter to affected individuals).

Mitigation (Section 9)	
	Component Privacy Office/PPOC works in consultation with the Component IT Security Entity, 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 Office/PPOC and Component IT Security Entity regarding containment measures.
	Component IT Security Entity and Component Privacy Office/PPOC manage and contain the incident.
	Component IT Security Entity and Component Privacy Office/PPOC implement actions to correct and prevent further risks stemming from the incident.
	Component Privacy Office/PPOC secures paper records, if applicable.
	Component IT Security Entity and Component Privacy Office/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 Office/PPOC restores security measures protecting paper information, if applicable.
	Component IT Security Entity and Component Privacy Office/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-GLD if criminal activity is suspected or confirmed and consultation to determine whether law enforcement should be notified; and □ Notification of the issuing bank for incidents involving credit cards (Sections 5 and 6).
	Component IT Security Entity and Component Privacy Office/PPOC document all implemented mitigation measures in the Privacy Incident Report.
Consequences and Accountability for Violation of Federal Laws, Regulations, or Directives, or DHS Policy (Section 10)	
	Component Privacy Office/PPOC informs the Component Head where DHS personnel have failed to implement safeguards to protect PII or where 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-GLD, and CHCO in the event that the Privacy Incident arises from violations or potential violations of the ethics statutes or regulations.
	Component Privacy Office/PPOC notifies the DHS OGC-GLD and Component Office of the Chief Counsel where DHS personnel (including employees, supervisors, and managers) fail to implement safeguards to protect PII or where 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-GLD or Component Office of the Chief Counsel consults with the Component Privacy Office/PPOC or other PIRT members, Component Head, and CHCO on legal issues pertaining to disciplinary or corrective action.
	Component Privacy Office/PPOC documents 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 Privacy Incidents (Section 11)	
	Component Privacy Office/PPOC and Component IT Security Entity update the incident report at https://soconline@dhs.gov to recommend incident closure, subject to review by the DHS CPO and DHS CIO.
	DHS CSIRC/SOC makes closure recommendation in weekly status reports of ongoing Privacy Incidents.
	Incident report is closed unless DHS CPO or DHS CIO notifies DHS SOC that the incident must remain open for review or further incident handling.
	DHS SOC automatically issues closure notifications to DHS Deputy Secretary, DHS CPO, DHS CIO, DHS Deputy CIO, DHS CISO, and DHS OGC-GLD.
Supplemental Activities (Sections 5.6, 8.1.2, 11, and 12)	
	DHS SOC issues weekly status report of ongoing incidents to senior management.
	PIRT or Component Privacy Office/PPOC (if no PIRT is convened) identifies and posts lessons learned in SOC Online Incident Handling System (https://soconline@dhs.gov).
	Component Privacy Office/PPOC collects and updates point of contact information concerning C-PIRT members, and provides the information to the DHS CPO, DHS CIO, and DHS CISO in a timely manner.
	DHS CPO collects and maintains point of contact information from DHS Components and from members of D-PIRT.
	D-PIRT convenes at least annually to review departmental implementation of Privacy Incident Handling Guidance.

Points of Contact for Privacy Incident Handling

The Points of Contact chart below should be completed by each Component and updated when necessary. Please provide a copy of the completed Point of Contact Chart to **DHSPrivacyIncident@dhs.gov** and provide updates as necessary.

	Name	Work Tel./Cell	Email
Component Help Desk			
Component ISSM			
Component Privacy Office/PPOC			
Component CSIRC/SOC			
DHS Help Desk	N/A	1-800-250-7911	itsupport@dhs.gov
DHS Chief Privacy Officer	Hugo Teufel III	703-235-0780	DHSPrivacyIncident@dhs.gov
DHS SOC	N/A	703-921-6505	dhs.soc@dhs.gov

Appendix D: Escalation Risk Assessment

(To be Prepared by the Component Privacy Office or PPOC)

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

The Component Privacy Office/PPOC should use this form as the 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 in this form (e.g., SSN, name, etc.). Upon completion of this form, upload it and any other relevant documents to the Privacy Incident Report in the DHS SOC Online Incident Handling System. Also send the assessment via email to: the Deputy Secretary, the DHS Privacy Office at DHSPrivacyIncident@dhs.gov, DHS CIO, and DHS CISO. If a PIRT is convened, email the assessment to all members.

This assessment should 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

Caution: Refer to facts stated in the Privacy Incident Report, but ensure that updated or supplemented facts are included in this section.

Specify data elements potentially at risk.	☐ Name ☐ Date of birth ☐ Mailing address ☐ Telephone number ☐ SSN ☐ 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 information was potentially compromised. State the media 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 implicates identity theft concerns, check the appropriate boxes. Indicate whether the incident involves any of the following data elements:

☐ SSN; **OR**

☐ A name, address, or telephone number, combined with:

- ☐ Any government-issued identification number (such as a driver's license number);
- ☐ Biometric record;
- ☐ Financial account number, together with a PIN or security code, if a PIN or security code is necessary to access the account; or
- ☐ Any additional, specific factor that adds to the personally identifying profile of a specific individual, such as a relationship with a specific financial institution or membership in a club.

Other types of PII are also useful in committing identity theft. State whether the incident involves:

☐ Date of birth ☐ Account Password ☐ 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 Sections 4 and 5.**

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. Assess the likely risk of harm in Section 3(b). Complete the table in Section 3(b), then proceed to Sections 4 and 5.

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 <u>limited or no</u> harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained; or

(2) Could have <u>limited or no</u> 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.

(3) The incident involves Sensitive PII (see PIHG Section 2.4.14.)

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.

(3) The incident involves Sensitive PII (see PIHG Section 2.4.14.)

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

Privacy Incidents That Do NOT Pose Risk of Identity Theft

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

Type of Factor	Identify Risk Level (e.g., Low, Moderate, High) and Provide Brief 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 the PII is accessible and usable	Is the information ☐ Electronic or ☐ Hardcopy? How difficult is it for an unauthorized person to access the information in light of the manner in which the information was protected? Was it locked or secured? Yes ☐ No ☐ If secured, identify what physical or electronic protections for electronic or hardcopy, if any, apply.

	What is the likelihood that an unauthorized individual will know the value of the information and either use the information or sell it to others? Summarize the risk.
Likelihood PII may lead to harm	Will substantial harm, embarrassment, inconvenience or unfairness occur from this loss? Yes ☐ No ☐ Explain why.
Ability to mitigate risk of harm	Explain the extent to which the agency has the capabilities to take countermeasures.

Section 3(b): Analysis of Risk: Five Factors **Privacy Incidents That Pose Risk of Identity Theft** **(Component Privacy Office/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 access the information 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 means the loss or compromise of PII occurred. • Was it the result of a criminal act (e.g., PII stolen targeting the data such as 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 Office/PPOC should categorize the incident as either a Moderate- or a High-Impact Privacy Incident. PIRT should be convened for incident handling. Under these circumstances, Component Privacy Office/PPOC, in coordination with Component SOC or DHS SOC Security Technical Support 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, DHS OIG, and DHS OGC-GLD. If criminal activity impacts physical security, the Component Privacy Office/PPOC, in coordination with Component SOC or DHS SOC Security Technical Support Officer, will ensure consultation and reporting with the Component CSO; Component CSO will determines whether to contact law enforcement (internal or external).**
Ability to mitigate risk of harm	Please explain the extent the agency has the capabilities to take countermeasures. Does the incident involve government-authorized credit cards? Yes ☐ No ☐ If so, has DHS notified the issuing bank? Yes ☐ No ☐ Does the incident involve individuals' bank account numbers used for the direct deposit of credit card reimbursements, government employee salaries, or any benefit payment? Yes ☐ No ☐ Has DHS notified the bank or other entity that handles that particular transaction for DHS? Yes ☐ No ☐

	Can DHS monitor and prevent attempts to misuse the covered information? Yes ☐ No ☐ Does the compromised information present a risk of new accounts being opened? Yes ☐ No ☐ If so, is data breach monitoring be appropriate (e.g., volume of persons affected or law enforcement evidence)? Yes ☐ No ☐ Would credit monitoring be more appropriate? Yes ☐ No ☐ Has the DHS OIG been notified? 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 Office or 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 Office/PPOC for Component experiencing incident ☐ C-PIRT: The Privacy Office/PPOC should convene C-PIRT to handle Moderate-impact Privacy Incidents **NOTE: If C-PIRT should handle the remaining stages of the incident, the Component Privacy Office/PPOC should immediately convene the C-PIRT**. ☐ D-PIRT: D-PIRT should be convened to handle High-Impact Privacy Incidents **NOTE: If the Component Privacy Office/PPOC recommends that a D-PIRT handle the remaining stages of the incident, the Component Privacy Office/PPOC should immediately inform the DHS Privacy Office.**	
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 immediately implemented).
Recommendation: preliminary assessment of whether external notification is warranted	Based upon the facts known at the time of escalation, make a preliminary recommendation whether external notification is warranted. **NOTE: The final decision regarding external notification will be made by:** • **The Chair of D-PIRT and the Component Head if a D-PIRT has been convened; or** • **The Chair of C-PIRT and the Component Head if a C-PIRT has been convened to handle the incident.** **If warranted, 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 internal notice to DHS senior officials must be given.**

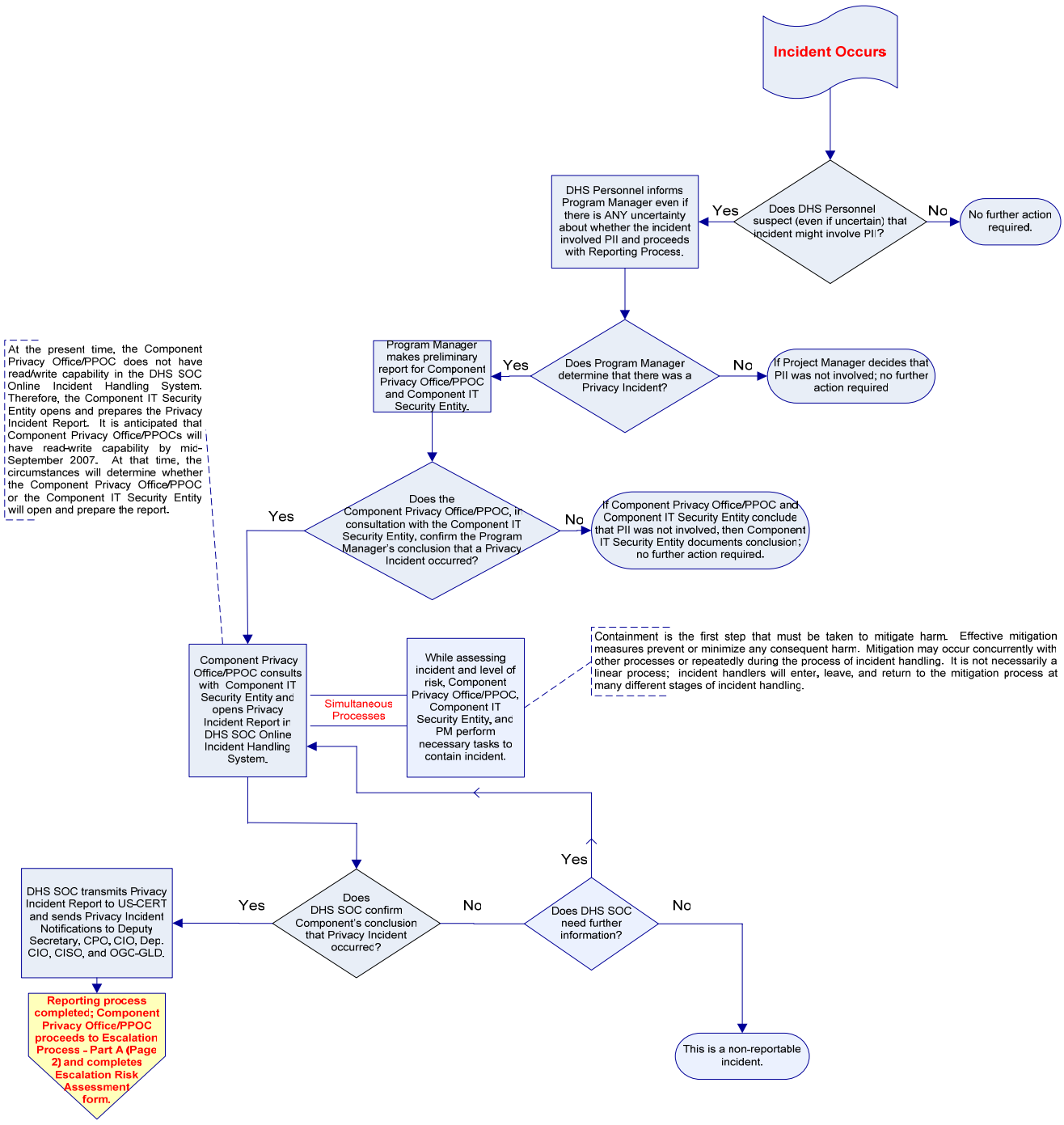
Section 5: D-PIRT's Plan of Action (to be completed by the DHS Privacy Office if D-PIRT is Recommended)		
Categorization of Privacy Incident	☐ Low ☐ Moderate ☐ High	If D-PIRT disagrees with the categorization of the incident, explain why.
Concur with recommendation to convene D-PIRT?	Yes ☐ No ☐ If not, explain why. **NOTE: The DHS CPO and other DHS senior officials will review the recommendation to convene a D-PIRT. If DHS senior officials concur with the recommendation, they will immediately convene D-PIRT and identify the Chair of D-PIRT of this particular the Privacy Incident.**	
Concur with suggested mitigation measures?	Yes ☐ No ☐ If not, please explain why.	
Notification Recommendation	**NOTE: PIRT should refer to and complete the External Notification Assessment, which outlines whether, how, and when notification should be**	

	provided, and identifies who should provide notification.

Section 6: C-PIRT's Plan of Action (to be completed by C-PIRT, if convened)		
Categorization of Privacy Incident	☐ Low ☐ Moderate ☐ High	If C-PIRT disagrees with the categorization of the incident, explain why.
Concur with suggested mitigation measures?	Yes ☐ No ☐ If not, explain why.	
Notification Recommendation	**NOTE: PIRT should refer to and complete the External Notification Assessment which outlines whether, how and when notification should be provided and identifies who should provide notification.**	

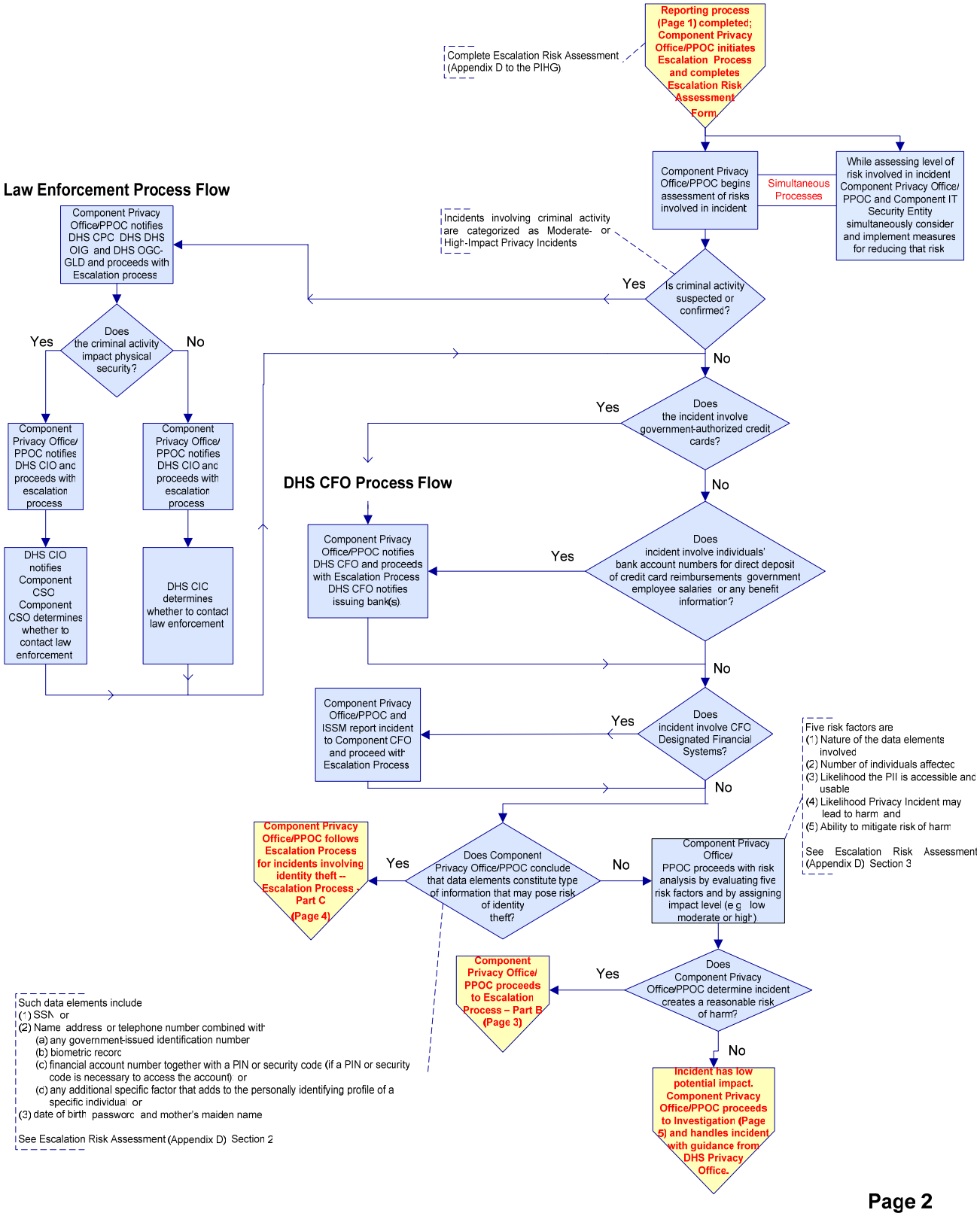
Appendix E: Process Flows for the Stages of Privacy Incident Handling

Privacy Incident Handling Guidance: Reporting Process (Section 5 of the PIHG)



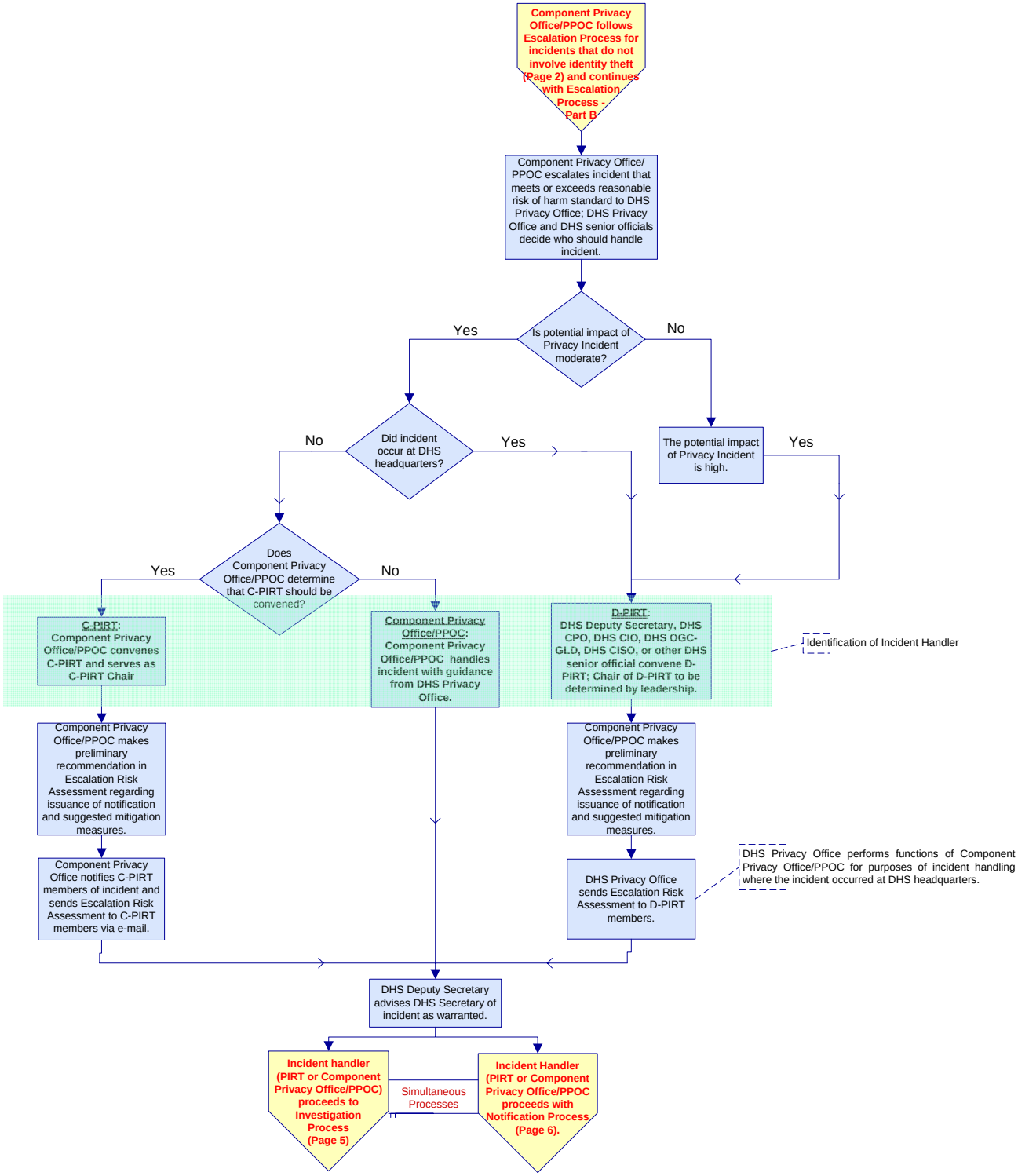
Page 1

Privacy Incident Handling Guidance:
Escalation Process Flow - Part A (Section 6 of the PIHG)



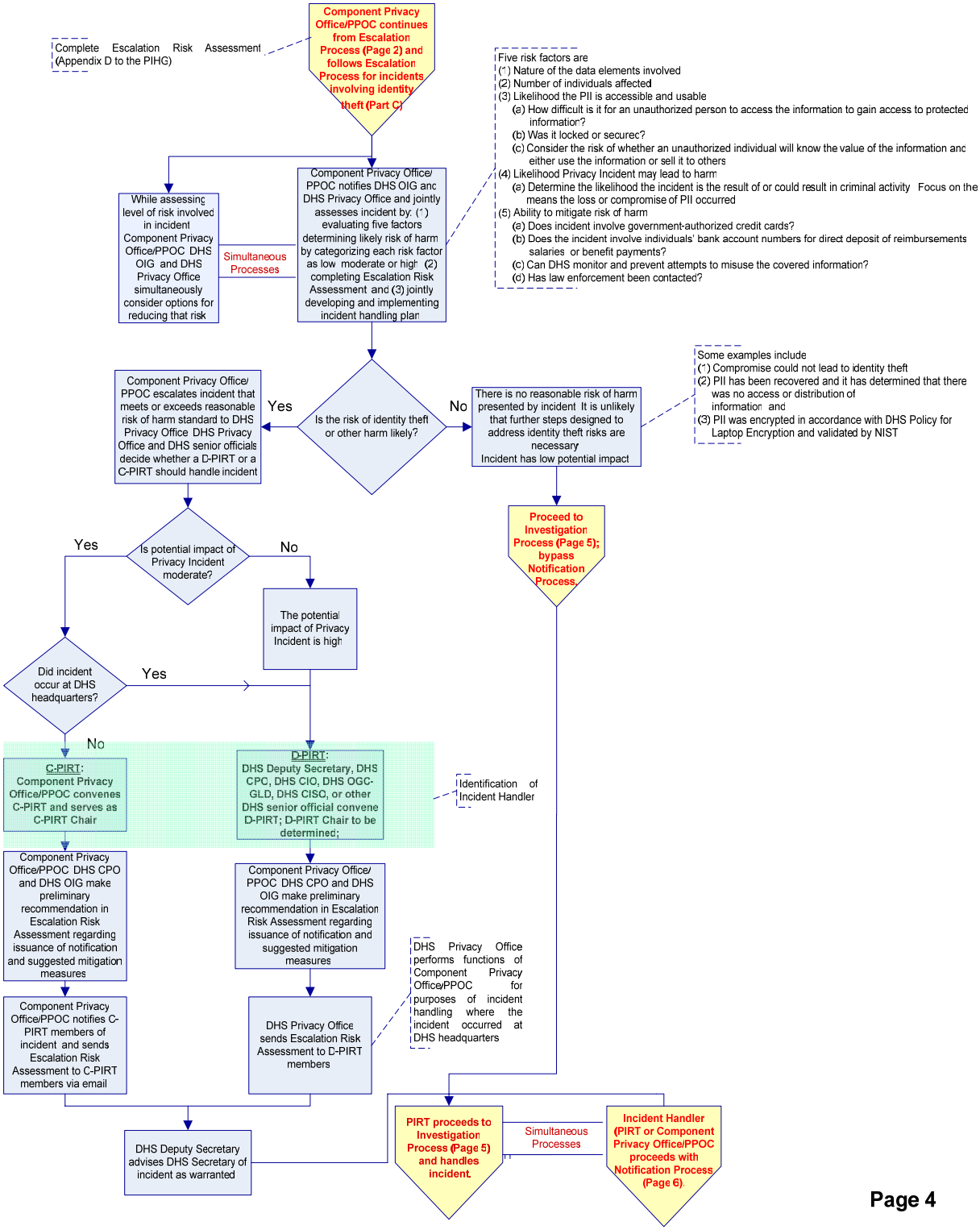
Page 2

Privacy Incident Handling Guidance:
Escalation for Incidents That Do Not Involve Risk of Identity Theft - Part B
(Section 6 of the PIHG)



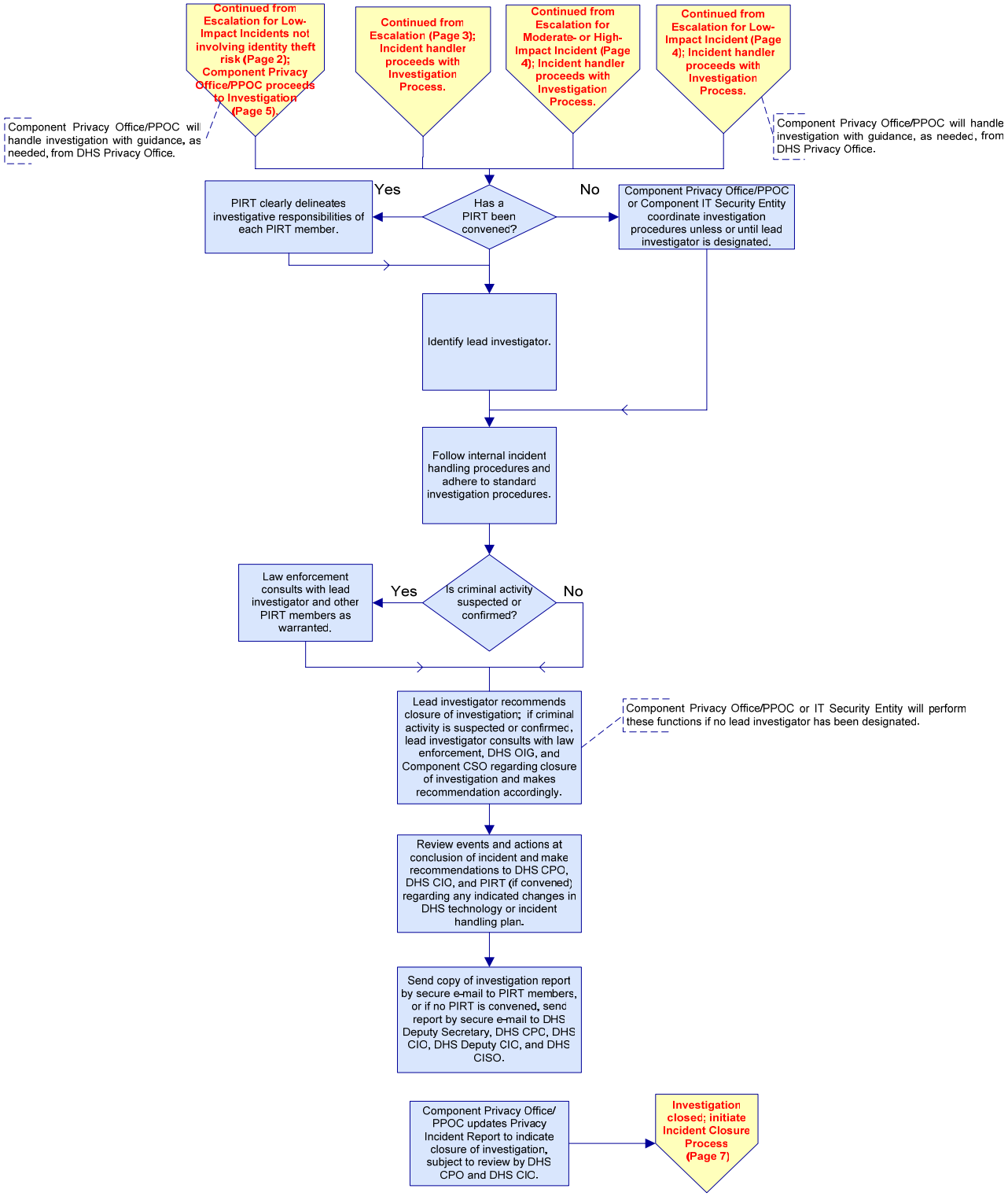
Page 3

Privacy Incident Handling Guidance:
Escalation for Incidents Involving Identity Theft Risk - Part C (Section 6.6 of the PIHG)



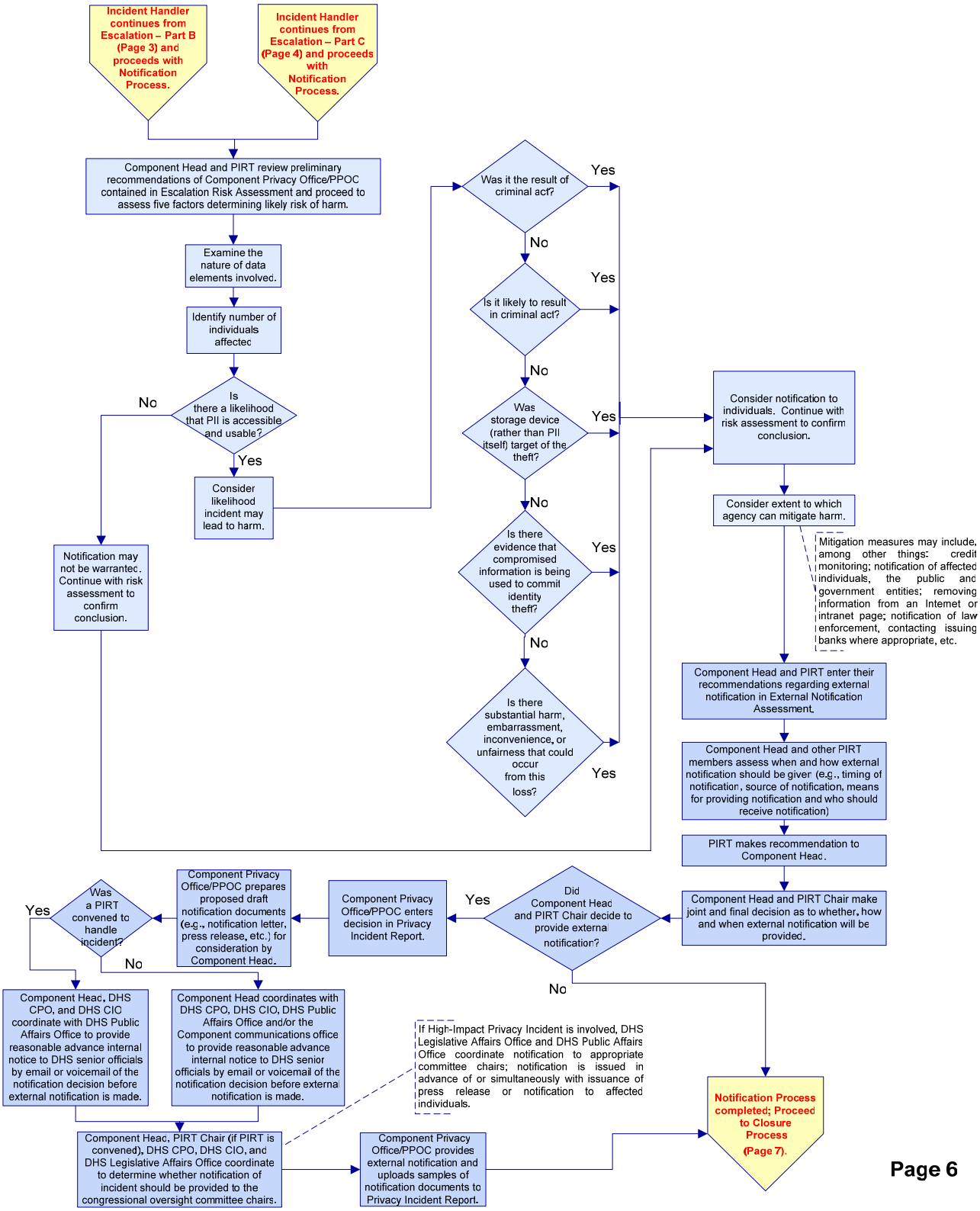
Page 4

Privacy Incident Handling Guidance:
Investigation (Section 7 of the PIHG)



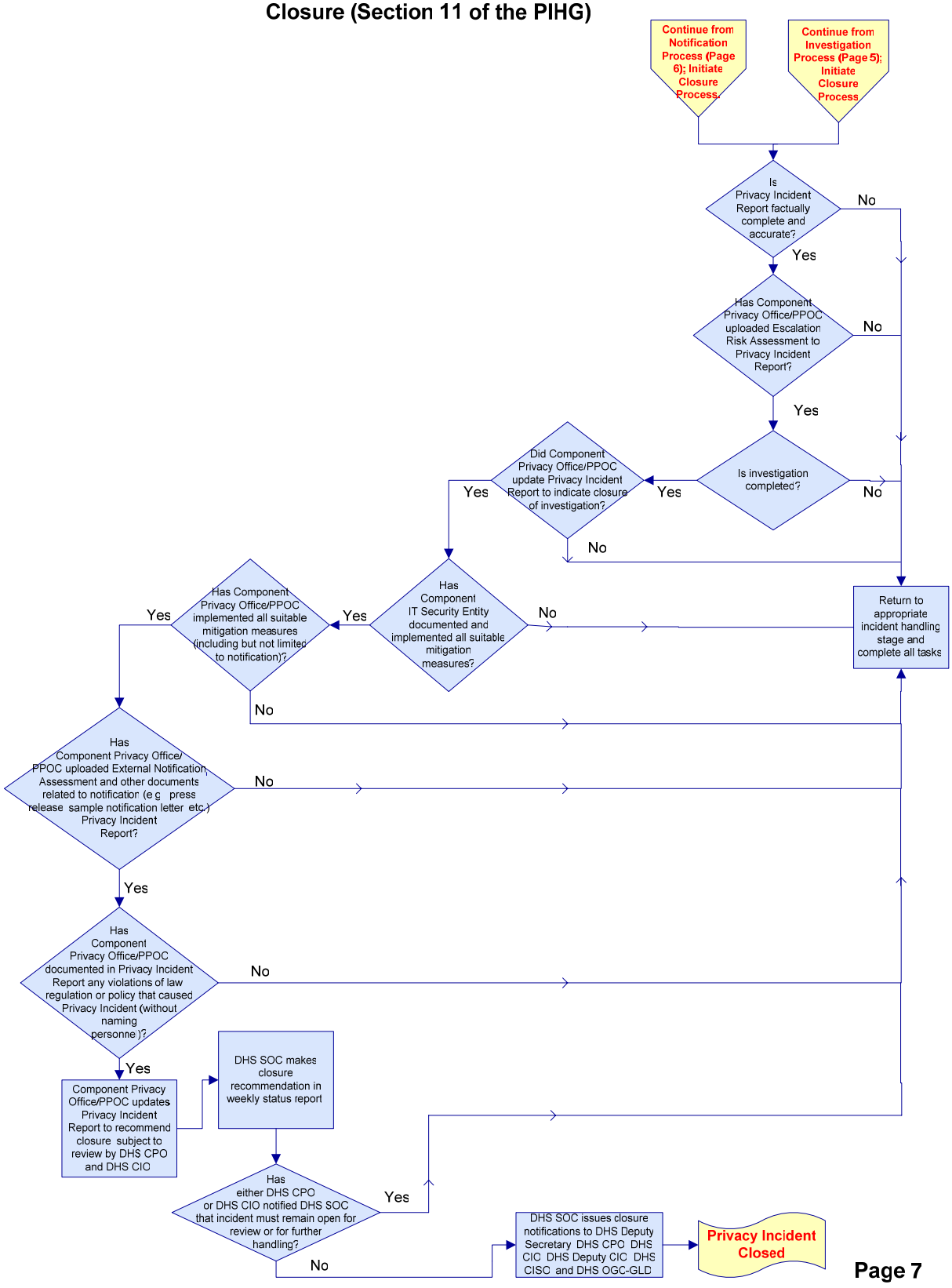
Page 5

Privacy Incident Handling Guidance:
Notification (Section 8 of the PIHG)



Page 6

Privacy Incident Handling Guidance: Closure (Section 11 of the PIHG)



Page 7

Appendix F: 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. **[If applicable, insert an explanation as to whether the Component Head of believes that the information will remain confidential]. [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.

Credit Reporting Firm	Telephone Number
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 account; and
2. Order a free credit report from the agency.

NOTE TO COMPONENT PRIVACY OFFICE/PPOC

Component must not make external notification to affected third parties without securing prior authorization from appropriate DHS senior officials. A decision to release public information will be a joint decision made by the Component Head and PIRT Chair.

No public release of information may be made unless and until *reasonable advance notice* is provided to the following DHS senior officials of DHS: the Offices of the Secretary and Deputy Secretary, the General Counsel, DHS CPO, DHS CIO, DHS Deputy CIO, DHS CISO, the CIO of the affected Component, and the DHS Public Affairs Office.

REMOVE THIS MESSAGE BEFORE DISTRIBUTION

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;
    - 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.consumer.gov/idtheft/.

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 one and the increasing number of data breaches 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]

Appendix G: Sample Press Release

[DATE]

FOR IMMEDIATE RELEASE

[COMPONENT NAME]
[COMPONENT LOGO]

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

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 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 OFFICE/PPOC

Component must not make external notification to affected third parties without securing prior authorization from appropriate DHS senior officials. A decision to release public information will be a joint decision made by the Component Head and PIRT Chair.

No public release of information may be made unless and until *reasonable advance notice* is provided to the following DHS senior officials of DHS: the Offices of the Secretary and Deputy Secretary, the General Counsel, DHS CPO, DHS CIO, DHS Deputy CIO, DHS CISO, the CIO of the affected Component, and the DHS Public Affairs Office.

REMOVE THIS MESSAGE BEFORE DISTRIBUTION

Appendix H: List of Acronyms

CFO – Chief Financial Officer

CFR – Code of Federal Regulations

CHCO – Chief Human Capital Officer

CIO – Chief Information Officer

CISO – Chief Information Security Officer

CONOPS – Concept of Operations

C-PIRT – Component Privacy Incident Response Team

CPO – Chief Privacy Officer

CSIRC – Computer Security Incident Response Center

CSO – Chief Security Office

DAA – Designed Accrediting Authority

DHS – Department of Homeland Security

D-PIRT – Departmental Privacy Incident Response Team

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

IRS – Internal Revenue Service

ISSM – Information Systems Security Manager

IT – Information Technology

MD – Management Directive

NIST – National Institute of Standards and Technology

OGC-GLD – Office of General Counsel, General Law Division

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

Pub – Publication

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

VA – Department of Veterans Affairs

VPN – Virtual Private Network