Homeland Security

DHS 4300A

Information Technology System Security Program, Sensitive Systems

Attachment V

Privacy Instruction

Version 1.0

July 29, 2022

Document Change History

Version	Date	Description
1.0	July 28, 2022	Initial version.

TABLE OF CONTENTS

1.0 INTRODUCTION

The DHS Privacy Office is responsible for privacy compliance across the Department, including assuring that technologies used by the Department sustain and do not erode privacy protections relating to the use of personal and Departmental information. The DHS Chief Privacy Officer has exclusive jurisdiction over the development of policy relating to personally identifiable information (PII) and to privacy-sensitive programs, systems, or initiatives.

2.0 SCOPE

This Instruction is meant to outline the privacy requirements that must be applied to all IT systems across the Department.

3.0 PRIVACY PROCESSES AND PROCEDURES

3.1 Personally Identifiable Information (PII) and Sensitive PII (SPII)

Various regulations place restrictions on the Government's collection, use, maintenance, and release of information about individuals. Regulations require agencies to protect PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the United States, or Department employee or contractor.

Sensitive PII (SPII) is PII which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Examples of SPII include Social Security numbers, A-number, medical information, and criminal history. The sensitivity of this data requires that stricter handling guidelines be applied. For more information on handling SPII see: *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information.*

Consistent with *Fair Information Practice Principles (FIPPs)*, PII collected and maintained by DHS should be accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in public notices. In addition, DHS adheres to data minimization and retention requirements to collect, use, and retain only PII that is relevant and necessary for the purpose for which it was originally collected. Programs should retain PII for only as long as necessary to fulfill the purpose(s) specified in public notices and in accordance with a record retention schedule approved by National Archives and Records Administration (NARA).

3.2 Privacy Compliance Documentation

The DHS Privacy Office works with Component Privacy Officers, Privacy Points of Contact (PPOC), Program Managers, System Owners, and information systems security personnel to

ensure that appropriate privacy practices and controls are integrated into the Department's operations. The DHS Privacy Office assesses the privacy risk of DHS IT systems and develops mitigation strategies by reviewing and approving all DHS privacy compliance documentation. The privacy compliance process is an ongoing cycle with four key parts to ensure appropriate oversight: Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA), System of Records Notice (SORN), and periodic review. Each part has a distinct function in implementing privacy policy at DHS, and together they enhance the oversight of and transparency into Department activities and demonstrate accountability to the public.

To promote privacy compliance within the Department, the Privacy Office has published official Department guidance regarding the requirements and content for privacy compliance documentation. Privacy Compliance Guidance can be found on the DHS Privacy Office website at www.dhs.gov/privacy.

3.2.1 Privacy Threshold Analysis (PTA)

A PTA provides a high-level description of an information system including the information it contains and how it is used. The PTA is used to determine and document whether or not a PIA and/or SORN are required. The first step in the process for DHS staff seeking to implement or update a system is to complete a PTA. The PTA is drafted and developed by Program Managers, System Owners, and information systems security personnel, then routed through the appropriate Component Privacy Office or PPOC, and then formally submitted to the DHS Privacy Office. The DHS Privacy Office reviews the PTA to determine if the system is privacy-sensitive and requires additional privacy compliance documentation such as a PIA or SORN. PTAs expire and must be reviewed and re-certified every three years or when changes/updates occur.

Privacy Policy and Compliance Directive 047-01 and Privacy Policy and Compliance Instruction 047-01-001 further outline PTA requirements, which are also listed below.

PTA Responsibilities
System/Program Owner Submits the PTA to the Component Privacy Officer or PPOC and provides any additional information required by the DHS Chief Privacy Officer to assist in the PTA process. **Component Privacy Officer or PPOC** Reviews and submits the PTA for approval and provides any additional information required by the DHS Chief Privacy Officer to assist in the PTA process. **DHS Chief Privacy Officer** Reviews and approves the PTA. Determines whether a system is a Privacy Sensitive System.

Determines whether a PIA and/or SORN are required.

3.2.2 Privacy Impact Assessment (PIA)

PIAs, which are publicly releasable documents, are required by the *E-Government Act of 2002, the Homeland Security Act of 2002*, and/or DHS Privacy policy. The PIA is a decision tool used by DHS to identify and mitigate privacy risks of systems, and inform the public (1) what PII DHS is collecting; (2) why the PII is being collected; and (3) how the PII will be collected, used, accessed, shared, safeguarded, and stored. PIAs assess risk by applying the universally recognized FIPPs to Department systems. PIAs are one tool that DHS uses to convey public notice of information practices and the privacy impact of Department programs and activities. The Department also uses web privacy policies, System of Records Notices, and Privacy Act Statements to provide effective public notice of program privacy practices. PIAs also document how DHS makes individuals active participants in the decision-making process regarding the collection and use of their PII.

PIAs are the responsibility of the System Owner and the Program Manager. If a PIA is required, the System Owner/Program Manager will work with the Component Privacy Office or POC to write the PIA for submission to the DHS Privacy Office for review and approval by the Chief Privacy Officer. PIAs must be approved and published before new PII may be collected.

OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, DHS Privacy Policy Guidance Memorandum 2008-02, Privacy Policy and Compliance Directive 047-01 and Privacy Policy and Compliance Instruction 047-01-001 further outline PIA requirements, which are also listed below.

PIA Responsibilities
System/Program Owner
Drafts accurate and complete PIA using DHS-approved templates.
Identifies, as part of the PIA, privacy risks and mitigation strategies.
Submits the draft PIA to the Component Privacy Officer or PPOC for review and comment.
Component Privacy Officer or PPOC
Reviews draft PIAs for possible privacy risks and mitigation strategies and works with System/Program Owners to address any privacy considerations associated with the system.
Submits the complete and accurate PIA for DHS Chief Privacy Officer review and approval.
Includes legal counsel in review of PIAs to ensure legal compliance.
DHS Chief Privacy Officer
Reviews information systems for privacy concerns.

Identifies privacy risks and develops, in coordination with the System/Program Owner and Component Privacy Office/PPOC, mitigation strategies to be documented in the PIA. Approves and signs all PIAs.

3.2.3 System of Record Notice (SORN)

The Privacy Act of 1974 requires a SORN when PII is maintained by a federal agency in a system of records and the PII is retrieved by a personal identifier. A system of records is "*a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual*". The SORN describes the categories of records and individuals in the system of record; the routine uses of the data; how individuals can gain access to records pertaining to them and correct errors. The term "system of records" is not synonymous with "information system" and can include paper as well as electronic records. SORNs can be written to cover the records in a single group of records or a single information system or they can be written to cover multiple groups of records or multiple information systems. Information systems that are considered a System of Records must keep an accurate accounting of disclosures of information shared outside of the system.

Information systems that are considered a system of record may not be designated operational until an appropriate SORN has been published in the *Federal Register* for 30 days.

OMB's *Privacy Act Implementation, Guidelines and Responsibilities* (July 9, 1975) and Circular A-130 - Appendix I, "Federal Agency Responsibilities for Maintaining Records About Individuals", and DHS's Privacy Policy and Compliance Directive 047-01 and Privacy Policy and Compliance Instruction 047-01-001 further outline SORN requirements, which are also listed below.

SORN Responsibilities
System/Program Owner Drafts accurate and complete SORN using DHS-approved templates. Submits the draft SORN to the Component Privacy Officer or PPOC for review and comment. **Component Privacy Officer or PPOC** Reviews draft SORN and works with System/Program Owners to address any privacy considerations associated with the system. Submits the complete and accurate SORN for DHS Chief Privacy Officer review and approval. Includes legal counsel in review of SORN to ensure legal compliance. **DHS Chief Privacy Officer**

Reviews, approves, and signs all SORNs.

3.2.4 Periodic Reviews

Once the PTA, PIA, and SORN are completed, they are reviewed periodically by the DHS Privacy Office (timing varies by document type and date approved). Each PTA is given an expiration date depending on the adjudication/determination made by the DHS Privacy Office. PIAs and SORNs are reviewed continuously upon PTA submissions. System Owners and Program Managers should adhere to the expiration dates documented in their adjudicated PTAs.

In addition, the DHS Privacy Office also employees Privacy Compliance Reviews (PCR). PCRS are both the process followed and the final document designed to provide a constructive mechanism to improve a program's ability to comply with existing privacy policy and compliance documentation, including PIAs, SORNs, formal agreements, such as Memoranda of Understanding or Memoranda of Agreement, or at the discretion of the Chief Privacy Officer.

DHS Privacy Policy Instruction 047-01-004 for Privacy Compliance Reviews further outlines the PCR process.

3.3 Privacy Incident Reporting

The DHS Privacy Office is responsible for implementing the Department's privacy incident response program based on requirements outlined in OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (January 2017). Through close collaboration, the DHS Chief Privacy Officer, the DHS CIO, the DHS CISO, the DHS ESOC, and Components ensure that all DHS privacy and computer security incidents are identified, reported, and appropriately responded to, in order to mitigate harm to DHS-maintained assets, information, and personnel. Incidents involving (or that may involve) PII are subject to strict reporting standards and timelines.

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

3.3.1 Privacy Incident Roles and Responsibilities

3.3.1.1 DHS Chief Privacy Officer

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

- Responsible for determining whether the Department's response can be conducted at the direction of the Component Privacy Officer/PPOC or whether the Chief Privacy Officer convenes the Breach Response Team (BRT). The Chief Privacy Officer may choose not to convene the BRT if the response can be conducted at the Component level. At a minimum, the BRT is convened when a privacy incident constitutes a "major incident," as defined by OMB.
- Leads and manages the BRT once convened.
- Refers all privacy incidents that may contain indicia of fraud, waste, and abuse to the Office of Inspector General.
- Evaluates the sensitivity of the PII involved in the privacy incident and assesses the risk of harm to individuals affected by the privacy incident.
- Directs BRT or Component Privacy Officer/PPOC to gather, analyze, and preserve any and all evidence necessary to support an investigation of a privacy incident, in accordance with Section 222 of the Homeland Security Act of 2002.
- Consults with the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) to determine whether a privacy incident constitutes a major incident pursuant to OMB M-18-02, Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management, and subsequent OMB Guidance, which may trigger Congressional reporting requirements under the FISMA.
- Provides recommendations for notification options to the Secretary after consultation with the BRT regarding a major privacy incident.
- Elevates issues to the Deputy Secretary if the BRT requires additional guidance or conflict resolution.

3.3.1.2 DHS Breach Response Team

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

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

3.3.1.3 DHS Privacy Office, Director of Privacy Incidents

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

- Notifies DHS SOC when an incident is closed, or if the incident will remain open for review or further incident handling.

3.3.1.4 DHS Chief Information Officer (DHS CIO)

- Provides management direction for the DHS SOC and overall direction for the responsible SOCs, and ensures oversight and compliance with DHS policy regarding privacy incident responses.
- Identifies, directs, and conducts technical remediation and forensic capabilities that exist within the Department and which offices are responsible for maintaining those capabilities, which provides technical support to respond to a privacy incident.
- Is a member of the BRT when convened.
- Evaluates the implementation and effectiveness of security safeguards when assessing the likelihood of access and use of PII compromised by a privacy incident.

3.3.1.5 DHS Chief Information Security Officer (DHS CISO)

- Oversees the DHS SOC, providing security oversight and information assurance for all DHS information systems, including assessing the risk and magnitude of harm to such systems resulting from a privacy incident.
- Briefs the CIO and other senior management officials on significant and major privacy incidents that impact availability, confidentiality, and integrity of network/system assets, provides the status of ongoing investigations, and the outcomes of completed investigations.
- Is a member of the BRT when convened.
- Ensures that incidents are reported to US-CERT in accordance with federal regulations and guidance, and approves of such reports prior to their release to external government entities.

3.3.1.6 DHS Security Operations Center (DHS SOC)

- Serves as a central repository and coordination point for privacy incidents within DHS.
- Reviews and evaluates the Privacy Incident Report for sufficiency, transmits such report to US-CERT within one hour of receipt from the Component Privacy Officer/PPOC or responsible SOC, and provides technical assistance as needed.
- Seeks approval to close any privacy incident from PRIV in cases involving PII.

3.3.1.7 Component Heads

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

3.3.1.8 Component Privacy Officers/PPOCs

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

3.3.1.9 Component Chief Information Officer

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

3.3.1.10 Responsible Security Operations Center (SOC)

- Recognize privacy incidents and understand the privacy incident reporting process and procedures.
- Consults with the Component Privacy Officer/PPOC regarding privacy issues affecting the security of information, assists the Component Privacy Officer/PPOC in preparing the Privacy Incident Report, investigates and remediates aspects of the

incident that impact computer security, and provides advice and assistance as needed.

- Provide advice, expertise, and assistance to BRT as needed.

3.3.1.11 DHS Personnel

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

3.3.1.12 DHS Supervisors and Program Managers

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

3.3.1.13 DHS Inspector General

- Consult with the DHS Chief Privacy Officer on a case-by-case basis to determine proper incident handling procedures for major privacy incidents.

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

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

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

The DHS Privacy Incident Handling Guidance (PIHG) further outlines privacy incident responsibilities. The PIHG is an instructional "roadmap" for responding to privacy incidents, addressing reporting to resolution of an incident, as well as developing lessons learned. This guidance describes the roles and responsibilities of DHS personnel, including employees, supervisors, Component Privacy Officers/PPOCs as well as the responsible Security Operations Center (SOC). All have a critical role at the outset in establishing facts that will be needed, not only to contain the privacy incident, but also to identify appropriate mitigations and lessons learned. The PIHG applies to all DHS personnel using, or with access to, DHS information and information systems in an unclassified environment in any format (e.g., paper, electronic). Although most incidents involve information technology, a privacy incident may also involve oral, paper, electronic, and physical security considerations that may cause the compromise of PII.

3.4 Use Limitation and External Information Sharing

Programs may use PII either as specified in public notices, in a manner compatible with those specified purposes, or as otherwise permitted by law. Sharing PII outside the Department is restricted to a purpose compatible with the purpose for which the PII was collected and in accordance with the routine uses in the applicable SORN.

DHS uses PII only for legally authorized purposes and in a manner compatible with uses identified in the Privacy Act or in other public notices. The DHS Chief Privacy Officer and, where appropriate, legal counsel review and approve any proposed external sharing of PII, including with other public, international, or private sector entities, for consistency with uses described in the

existing privacy compliance documentation such as PIAs and SORNs or other public notice(s). When a proposed new instance of external sharing of PII is not currently authorized by the Privacy Act or specified in a notice, the Chief Privacy Officer evaluates whether the proposed external sharing is compatible with the purpose(s) specified in the notice. If the proposed sharing is compatible, program owners review, update, and republish their PIAs, SORNs, website privacy policies, and other public notices, if any, to include specific descriptions of the new uses(s) and obtain consent where appropriate and feasible. Information sharing agreements also include security protections consistent with the sensitivity of the information being shared.

DHS programs that engage in Computer Matching Agreements (CMA) follow established DHS guidance for ensuring that controls are in place to maintain both the quality and integrity of data shared under CMAs. These responsibilities are further outlined in Computer Matching Agreements and the Data Integrity Board Directive 262-01 and Computer Matching Agreements and the Data Integrity Board Instruction 262-01-001.

4.0 GLOSSARY

Fair Information Practice Principles means the policy framework adopted by the Department regarding the collection, use, maintenance, disclosure, deletion, or destruction of Personally Identifiable Information.

Individual means a natural person, including a United States citizen, Legal Permanent Resident, visitor to the United States, noncitizen, DHS employee, or DHS contractor. C

Information Sharing Agreement (ISA) means an agreement that defines the terms and conditions of information/data exchanges between two or more parties. ISA encompasses agreements in any form, including Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, etc.

Personally Identifiable Information (PII) means any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual. For example, when linked or linkable to an individual, such information includes a name, social security number, date and place of birth, mother's maiden name, account number, license number, vehicle identifier number, license plate number, device identifier or serial number, internet protocol address, biometric identifier (e.g., photograph, fingerprint, iris scan, voice print), educational information, financial information, medical information, criminal or employment information, information created specifically to identify or authenticate an individual (*e.g.,* a random generated number).

Privacy Compliance Documentation means any document required by statute or by the Chief Privacy Officer that supports compliance with DHS privacy policy, procedures, or requirements, including but not limited to Privacy Threshold Analyses, Privacy Impact Assessments, System of Records Notices, Notices of Proposed Rulemaking for Exemption to Privacy Act System of Records (NPRM), and Final Rules.

Privacy Impact Assessment (PIA) means both the DHS Privacy Office process to be followed and the document required whenever an IT system, technology, rulemaking, program, pilot project, or other activity involves the planned use of PII or otherwise impacts the privacy of individuals as determined by the Chief Privacy Officer. A PIA describes what information DHS is collecting, why the information is being collected, how the information will be used, stored, and shared, how the information may be accessed, how the information will be protected from unauthorized use or disclosure, and how long it will be retained. A PIA also provides an analysis of the privacy considerations posed and the steps DHS has taken to mitigate any impact on privacy. As a general rule, PIAs are public documents. The Chief Privacy Officer may modify or waive publication for security reasons, or to protect classified, sensitive, or private information included in a PIA.

Privacy Incident means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users have access or potential access to PII in usable form, whether paper or electronic, or where authorized users access PII for an unauthorized purpose. Privacy Incidents include both suspected and confirmed incidents involving PII. K

Privacy Threshold Analysis (PTA) means both the DHS Privacy Office process to be followed and the document used to identify information technology (IT) systems, technologies, rulemakings, programs, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer, and to assess whether there is a need for additional Privacy Compliance Documentation. A PTA includes a general description of the IT system, technology, rulemaking, program, pilot project, or other Department activity and describes what PII is collected (and from whom) and how that information is used.

Program Manager means the DHS employee who is responsible for the planning and operation of a DHS program.

Sensitive Personally Identifiable Information (Sensitive PII) means PII which, if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an Individual. Some types of PII, such as Social Security Number (SSN), A-Number, and biometric identifiers, are always sensitive. Other types of PII, such as an individual's driver's license number, financial account number, citizenship or immigration status, or medical information are Sensitive PII if DHS maintains them in conjunction with other identifying information about the Individual. In some instances, the context surrounding the PII may determine whether it is sensitive. For example, a list of employee names by itself may not be Sensitive PII, but could be if it is a list of employees who received poor performance ratings.

System Manager means the DHS employee identified in a System of Records Notice who is responsible for the operation and management of the system to which the System of Records Notice pertains.

System of Records Notice (SORN) means the official public notice of a DHS system of records as required by the Privacy Act of 1974 (as amended). The SORN identifies (1) the purpose for the

system of records, (2) the individuals covered by information in the system of records, (3) the categories of records maintained about individuals, and (4) the ways in which the information is generally shared by the Department. The SORN also provides notice of the mechanisms available for individuals to exercise their Privacy Act rights to access and correct the PII that DHS maintains about them.

5.0 REFERENCES

Federal Laws

- Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"
- Office of Management and Budget (OMB) M-18-02, Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management
- OMB Memorandum M-17-12
- Preparing for and Responding to a Breach of Personally Identifiable Information (Jan 2017)
- OMB Circular A-130 Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals
- OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
- Fair Information Practice Principles (FIPPs)

Department of Homeland Security Publications

- Computer Matching Agreements and the Data Integrity Board Directive Number 262-01
- DHS Privacy Policy Instruction 047-01-004 for Privacy Compliance Reviews
- 4300A – The Sensitive Systems Handbook
- DHS Privacy Policy Compliance Directive 047-01
- DHS Privacy Policy and Compliance Instruction 047-01-001
- DHS Privacy Policy Guidance Memorandum 2008-02

6.0 ACRONYMS

Acronym	Meaning
AV	Anti-virus
BRT	Breach Response Team
CBP	Custom Boarder Protection
AO	Authorizing Official
BRT	Breach Response Team
ESOC	Enterprise Security Operations Center
FIPP	Fair Information Practice Principles
FISMA	Federal Information Security Management Act
HSAR	Homeland Security Acquisition Regulation
NARA	National Archives and Records
PCR	Privacy Compliance Review
PIA	Privacy Impact Assessment
PIHG	Privacy Incident Handling Guidance
PII	Personally Identifiable Information
PPOC	Privacy Points of Contact
PTA	Privacy Threshold Analysis
SOC	Security Operations Center
SORN	System of Record Notice
SPII	Sensitive Personally Identifiable Information