FIRST RESPONDER COMMUNITIES OF PRACTICE (FR COP) (SAT-05206-MAJ-05206)

System Privacy Plan (SPP)

Prepared for

Department of Homeland Security Headquarters (DHS HQ)
[Component address not provided]

Prepared by

Department of Homeland Security Headquarters (DHS HQ)

7 March 2018

(Content Version – 2014)

DOCUMENT CHANGE HISTORY

Version	Date	Author	Description

Preface

This system privacy plan (SPP) was developed by Department of Homeland Security Privacy Office. This plan is based upon a review of the system, documentation, DHS regulations/guidance, and interviews with the information system and privacy personnel. The SPP documents the applicability and compliance status of the NIST SP 800-53 Rev. 4 Appendix J Privacy Controls. DHS privacy personnel consulted with other DHS agency officials, including program mangers/information system owners, Authorizing Officials, Chief Information Officers, and Chief Information Security Officers to determine compliance with the applicable privacy controls for this system.

SAOP approval of the privacy controls is required as a precondition for the issuance of an authorization to operate (OMB M-14-04).

TABLE OF CONTENTS

LIST OF TABLES

1.0 System Identification and Information Security Posture

This System Privacy Plan (SPP) details the applicable privacy controls for FIRST RESPONDER COMMUNITIES OF PRACTICE (FR COP) and describes controls in place or planned for implementation. The SPP differs from the System Security Plan (SSP) which includes user responsibilities, roles and limitations, and general security procedures for users and security personnel. This section describes basic security information for the system. For a comprehensive description of the applicable system security controls, see the corresponding SSP.

1.1 System Name

Table 1-1 System Name

FISMA ID:	SAT-05206-MAJ-05206
System Name:	FIRST RESPONDER COMMUNITIES OF PRACTICE
System Abbreviation:	FR COP
Version:	1

1.2 Information Categorization

This section summarizes the FR COP information security categorization levels as determined by the FIPS 199 Information Security Categorization. The FR COP security impact levels for each of the three security objectives of confidentiality, integrity, and availability are identified in Table 1-2.

Table 1-2 Security Categorization

Confidentiality Impact Level:	Moderate
Integrity Impact Level:	Moderate
Availability Impact Level:	Low

Table 1-3 System Designations

Chief Financial Officer (CFO) Designated Financial System	No
System Contains Privacy Data or PII	Yes
Classification or Sensitivity Level	UNCLASSIFIED//FOUO
Mission Essential System	No

1.3 Privacy Controls Compliance

This table provides an at-a-glance of the FR COP compliance with the privacy controls. For a detailed description of the controls and compliance status, see each individual control below.

Table 1-4 Privacy Controls Compliance At-A-Glance

Test Title	Associated Control	Result	Notes
AP-1.1 - Authority to Collect	PRIV-AP-1	Passed	
AP-2.1 - Purpose Specification	PRIV-AP-2	Passed	
AR-1.1 - Governance and Privacy Program	PRIV-AR-1	Passed	
AR-2.1 - Privacy Impact and Risk Assessment	PRIV-AR-2	Passed	
AR-3.1 - Privacy Requirements for Contractors and Service Providers	PRIV-AR-3	Passed	
AR-4.1 - Privacy Monitoring and Auditing	PRIV-AR-4	Passed	
AR-5.1 - Privacy Awareness and Training	PRIV-AR-5	Passed	
AR-6.1 - Privacy Reporting	PRIV-AR-6	Passed	
AR-7.1 - Privacy-Enhanced System Design and Development	PRIV-AR-7	Passed	
AR-8.1 - Accounting of Disclosures	PRIV-AR-8	Passed	
DI-1.1 - Data Quality	PRIV-DI-1	Passed	
DI-2.1 - Data Integrity and Data Integrity Board	PRIV-DI-2	Passed	
DM-1.1 - Minimization of Personally Identifiable Information	PRIV-DM-1	Passed	
DM-2.1 - Data Retention and Disposal	PRIV-DM-2	Passed	
DM-3.1 - Minimization of PII Used in Testing, Training, and Research	PRIV-DM-3	Passed	
IP-1.1 – Consent	PRIV-IP-1	Passed	
IP-2.1 - Individual Access	PRIV-IP-2	Passed	
IP-3.1 – Redress	PRIV-IP-3	Passed	

IP-4.1 - Complaint Management	PRIV-IP-4	Passed	
SE-1.1 - Inventory of Personally Identifiable Information	PRIV-SE-1	Passed	
SE-2.1 - Privacy Incident Response	PRIV-SE-2	Passed	
TR-1.1 - Privacy Notice	PRIV-TR-1	Passed	
TR-2.1 - System of Records Notices and Privacy Act Statements	PRIV-TR-2	Passed	
TR-3.1 - Dissemination of Privacy Program Information	PRIV-TR-3	Passed	
UL-1.1 - Internal Use	PRIV-UL-1	Passed	
UL-2.1 - Information Sharing with Third Parties	PRIV-UL-2	Passed	

2.0 Controls

2.1	Authority to Collect	PRIV-AP-1
	Control: Authority to Collect The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need. Supplemental Guidance Before collecting PII, the organization determines whether the contemplated collection of PII is legally authorized. Program officials consult with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and legal counsel regarding the authority of any program or activity to collect PII. The authority to collect PII is documented in the System of Records Notice (SORN) and/or Privacy Impact Assessment (PIA) or other applicable documentation such as Privacy Act Statements or Computer Matching Agreements. Related controls: AR-2, DM-1, TR-1, TR-2. References: The Privacy Act of 1974, 5 U.S.C. § 552a (e); Section 208(c), E-Government Act of 2002 (P.L. 107-347); OMB Circular A-130, Appendix I.	
	Implementation: See SORN section "Authority for maintenance of the system" and PIA section 1.1 requires that Systems/Program owners list all statutory and regulatory authority for operating the project, including the authority to collect the information listed in PIA question 2.1. Systems/Program owners must explain how the statutory and regulatory authority permits collection and use of the information. A simple citation without more information will not be sufficient for purposes of this document and will result in rejection of a Privacy Impact Assessment. Systems/Program owners must explain how the statutory and regulatory authority permits the project and the collection of the subject information. If the project collects Social Security numbers, identify the specific statutory authority allowing such collection. If relying on another component and/or agency, please list their legal authorities. Where information is received from a foreign government pursuant to an international agreement or memorandum of understanding, cite the agreement and where it can be found (e.g. website). Responsible Entitles: System/Program Owner	
	Implementation Status: Implemented	Note: INSERTPIA and INSERTSORN complete and on file with DHS PRIV.

2.2	Purpose Specification	PRIV-AP-2
	Control: Purpose Specification The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices. Supplemental Guidance Often, statutory language expressly authorizes specific collections and uses of PII. When statutory language is written broadly and thus subject to interpretation, organizations ensure, in consultation with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and legal counsel, that there is a close nexus between the general authorization and any specific collection of PII. Once the specific purposes have been identified, the purposes are clearly described in the related privacy compliance documentation, including but not limited to Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), and Privacy Act Statements provided at the time of collection (e.g., on forms organizations use to collect PII). Further, in order to avoid unauthorized collections or uses of PII, personnel who handle PII receive training on the organizational authorities for collecting PII, authorized uses of PII, and on the contents of the notice. Related controls: AR-2, AR-4, AR-5, DM-1, DM-2, TR-1, TR-2, UL-1, UL-2. References: The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3)(A)-(B); Sections 208(b), (c), E-Government Act of 2002 (P.L. 107-347).	
	Implementation: See SORN section "Purpose" and any corresponding Privacy Act Statements which inform each individual whom the System/Program asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual: (A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary; (B) the principal purpose or purposes for which the information is intended to be used; (C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and (D) the effects on him, if any, of not providing all or any part of the requested information. Responsible Entitles: System/Program Owner	
	Implementation Status: Implemented	Note: INSERTPIA and INSERTSORN complete and on file with DHS PRIV.
2.3	Governance and Privacy Program	PRIV-AR-1
	Control: Governance and Privacy Program The organization: (a) Appoints a Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and information systems; (b) Monitors federal privacy laws and policy for changes that affect the privacy program; (c) Allocates DHS and Component Privacy Offices sufficient resources to implement and operate the organization-wide privacy program; (d) Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures; (e) Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and (f) Updates privacy plan, policies, and procedures PIAs updated every 3 years or when a change happens. SORNs every 2 years or when a change happens. Supplemental Guidance The development and implementation of a comprehensive governance and privacy program demonstrates organizational accountability for and commitment to the protection of individual privacy. Accountability begins with the appointment of an SAOP/CPO with the authority, mission, resources, and responsibility to develop and implement a multifaceted privacy program. The SAOP/CPO, in consultation with legal counsel, information security officials, and others as appropriate: (i) ensures the development,	

	implementation, and enforcement of privacy policies and procedures; (ii) defines roles and responsibilities for protecting PII; (iii) determines the level of information sensitivity with regard to PII holdings; (iv) identifies the laws, regulations, and internal policies that apply to the PII; (v) monitors privacy best practices; and (vi) monitors/audits compliance with identified privacy controls. To further accountability, the SAOP/CPO develops privacy plans to document the privacy requirements of organizations and the privacy and security controls in place or planned for meeting those requirements. The plan serves as evidence of organizational privacy operations and supports resource requests by the SAOP/CPO. A single plan or multiple plans may be necessary depending upon the organizational structures, requirements, and resources, and the plan(s) may vary in comprehensiveness. For example, a one-page privacy plan may cover privacy policies, documentation, and controls already in place, such as Privacy Impact Assessments (PIA) and System of Records Notices (SORN). A comprehensive plan may include a baseline of privacy controls selected from this appendix and include: (i) processes for conducting privacy risk assessments; (ii) templates and guidance for completing PIAs and SORNs; (iii) privacy training and awareness requirements; (iv) requirements for contractors processing PII; (v) plans for eliminating unnecessary PII holdings; and (vi) a framework for measuring annual performance goals and objectives for implementing identified privacy controls. Related control: None. References: The Privacy Act of 1974, 5 U.S.C. § 552a; E-Government Act of 2002 (P.L. 107-347); Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; OMB Memoranda 03-22, 05-08, 07-16; OMB Circular A-130; Federal Enterprise Architecture Security and Privacy Profile.
	Implementation: (a) The DHS Chief Privacy Officer, a statutorily mandated position by Section 222 of the Homeland Security Act (6 U.S.C. § 142), serves as the DHS Senior Agency Official for Privacy (SAOP) and reports directly to the Secretary of Homeland Security. Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001 the DHS Chief Privacy Officer is responsible for all aspects of the privacy governance program at the Department, including establishing, overseeing the implementation of, and issuing guidance on DHS privacy policy; and ensuring that the Department's use of technology sustains, and does not erode, privacy protections relating to the collection, use, maintenance, disclosure, deletion, and/or destruction of PII. (b) Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001 the DHS Chief Privacy Officer is responsible for ensuring that the Department follows privacy laws applicable to DHS, and federal government-wide privacy policies in collecting, using, maintaining, disclosing, deleting, and/or destroying PII. (c) The DHS Privacy Office allocates, through the annual appropriations process, sufficient resources to implement and operate the organization-wide privacy program. (d) The strategic goals and objectives of the DHS Chief Privacy Officer are detailed in the Privacy Office "FY 2012-2015 Strategic Plan," DHS Directive 047-01 "Privacy Policy and Compliance"" and Instruction 047-01-001. (e) DHS Privacy Office publishes policies and procedures as needed to ensure that Department technology sustains and does not erode, privacy protections relating to the collection, use, maintenance, disclosure, deletion, and/or destruction of PII. In addition to the comprehensive DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001, the DHS Privacy Office has published policies governing the appropriate privacy and security controls for programs, information systems, or technologies involving PII on the publicly available website, www.dhs.gov/privacy. Examples include: Privacy Policy Guidance Memorandum 2011-02, "Department policy establishing a formal Department-wide approach to the roles and responsibilities accompanying the cross-component sharing of IT services" (June 30, 2011); Privacy Policy Guidance Memorandum 2008-01, "The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security," (December 29, 2008); and Privacy Policy Guidance Memorandum 2007-02, "Regarding the use of Social Security numbers at the Department of Homeland Security," (June 4, 2007), and DHS MD 110-01, "Privacy Policy for Operational Use of Social Media," and corresponding Instruction (June 8, 2012). (f) Pursuant to the authority of the DHS Chief Privacy Officer in Section 222 of the Homeland Security Act (6 U.S.C. § 142), the DHS Privacy Office updates privacy plans, policies, and procedures on an as needed and continual basis, but at least biennially. Responsible Entitles: (a) DHS Chief Privacy Officer (b) DHS Chief Privacy Officer (c) DHS Chief Privacy Officer (d) DHS Chief Privacy Officer (e) DHS Chief Privacy Officer (f) DHS Chief Privacy Officer

	Implementation Status: Implemented	Note: INSERTPIA and INSERTSORN complete and on file with DHS PRIV.
2.4	Privacy Impact and Risk Assessment	PRIV-AR-2

Control: Privacy Impact and Risk Assessment

The organization:

(a) Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and
(b) Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

Supplemental Guidance

Organizational privacy risk management processes operate across the life cycles of all mission/business processes that collect, use, maintain, share, or dispose of PII. The tools and processes for managing risk are specific to organizational missions and resources. They include, but are not limited to, the conduct of PIAs. The PIA is both a process and the document that is the outcome of that process. OMB Memorandum 03-22 provides guidance to organizations for implementing the privacy provisions of the E-Government Act of 2002, including guidance on when PIAs are required for information systems. Some organizations may be required by law or policy to extend the PIA requirement to other activities involving PII or otherwise impacting privacy (e.g., programs, projects, or regulations). PIAs are conducted to identify privacy risks and identify methods to mitigate those risks. PIAs are also conducted to ensure that programs or information systems comply with legal, regulatory, and policy requirements. PIAs also serve as notice to the public of privacy practices. PIAs are performed before developing or procuring information systems, or initiating programs or projects, that collect, use, maintain, or share PII and are updated when changes create new privacy risks.

Related control: None.

References: Section 208, E-Government Act of 2002 (P.L. 107-347); Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; OMB Memoranda 03-22, 05-08, 10-23.

Implementation: (a) Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001, the Chief Privacy Officer is responsible for the entire privacy risk management framework including (1) Establishing, overseeing the implementation of, and issuing guidance on DHS privacy policy; (2) ensuring in coordination with Component heads and Component Privacy Officers and Privacy Points of Contact (PPOC), that the Department follows DHS privacy policy, privacy laws applicable to DHS, and federal government-wide privacy policies in collecting, using, maintaining, disclosing, deleting, and/or destroying PII, and in implementing any other activity that impacts the privacy of individuals; (3) Ensuring that the Department's use of technology sustains, and does not erode, privacy protections relating to the collection, use, maintenance, disclosure, deletion, and/or destruction of PII; (4) Evaluating Department regulations, rulemakings, technologies, policies, procedures, guidelines, programs, projects, or systems (including pilot activities), whether proposed or operational, for potential privacy impacts and advising DHS leadership and Components on implementing corresponding privacy protections.

The PTA process identifies when privacy compliance documentation and subsequent notices require an update. The Chief Privacy Officer schedules completed PTAs, PIAs, and SORNs for mandatory review as follows: at least every three years for PTAs and PIAs, and every two years for SORNs. The Chief Privacy Officer notifies the relevant Component Privacy Officer or PPOC that a PTA, PIA, and/or SORN review is required and begins the collaborative review process, which follows the process described in this Instruction for new PTAs, PIAs, and SORNs.

(b) Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001 and DHS privacy policy memorandum 2008-02, the DHS Chief Privacy Officer conducts Privacy Impact Assessments (PIAs) under four specific statutory authorities. (1) Section 208 of the E-Government Act of 20021 requires PIAs of all information technology that uses, maintains, or disseminates personally identifiable information (PII) or when initiating a new collection of PII from ten or more individuals in the public. (2) Congress requires the Chief Privacy Officer to conduct PIAs on certain programs and activities of the Department. (3) Section 222(a)(4) of the Homeland Security Act of 2002, as amended,2 authorizes the Chief Privacy Officer to conduct PIAs on rulemakings proposed by DHS. (4) Section 222(a)(1) of the Homeland Security Act authorizes the Chief Privacy Officer to ensure that technologies employed at DHS sustain, and do not erode, privacy protections.

Responsible Entitles: (a) DHS Chief Privacy Officer
(b) System/Program Owner

	Implementation Status: Implemented	Note: INSERTPIA and INSERTSORN complete and on file with DHS PRIV.
2.5	Privacy Requirements for Contractors and Service Providers	PRIV-AR-3
	Control: Privacy Requirements for Contractors and Service Providers The organization: (a) Establishes privacy roles, responsibilities, and access requirements for contractors and service providers; and (b) Includes privacy requirements in contracts and other acquisition-related documents. Supplemental Guidance Contractors and service providers include, but are not limited to, information providers, information processors, and other organizations providing information system development, information technology services, and other outsourced applications. Organizations consult with legal counsel, the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO), and contracting officers about applicable laws, directives, policies, or regulations that may impact implementation of this control. Related control: AR-1, AR-5, SA-4. References: The Privacy Act of 1974, 5 U.S.C. § 552a(m); Federal Acquisition Regulation, 48 C.F.R. Part 24; OMB Circular A-130.	
	Implementation: (a) DHS adheres to the requirements in the Federal Acquisition Regulations, subpart 24.1. In addition, the Chief Privacy Officer determines privacy policy and standards for the Department consistent with the FIPPs; oversees compliance with DHS privacy policy, privacy laws applicable to DHS, and federal government-wide privacy policies; provides privacy guidance and training to DHS personnel regarding the FIPPs; and provides support on privacy-related matters to senior Department leadership and to the Components. (b) Per DHS Sensitive Systems Policy 4300A, subjection 3.3.j, all statements of work, contract vehicles, and other acquisition-related documents shall include privacy requirements and establish privacy roles, responsibilities, and access requirements for contractors and service providers. In addition, DHS adheres to the requirements in the Federal Acquisition Regulations, subpart 24.1. Responsible Entitles: (a) DHS Chief Privacy Officer (b) System/Program Owner	
	Implementation Status: Implemented	Note: INSERTPIA and INSERTSORN complete and on file with DHS PRIV.
2.6	Privacy Monitoring and Auditing	PRIV-AR-4
	Control: Privacy Monitoring and Auditing The organization monitors and audits privacy controls and internal privacy policy Depends. PTA, PIA, and SORN process evaluates some. Privacy compliance reviews are done as directed by DHS to ensure effective implementation. Supplemental Guidance To promote accountability, organizations identify and address gaps in privacy compliance, management, operational, and technical controls by conducting regular assessments (e.g., internal risk assessments). These assessments can be self-assessments or third-party audits that result in reports on compliance gaps identified in programs, projects, and information systems. In addition to auditing for effective implementation of all privacy controls identified in this appendix, organizations assess whether they: (i) implement a process to embed privacy considerations into the life cycle of personally identifiable information (PII), programs, information systems, mission/business processes, and technology; (ii) monitor for changes to applicable privacy laws, regulations, and policies; (iii) track programs, information systems, and applications that collect and maintain PII to ensure compliance; (iv) ensure that access to PII is only on a need-to-know basis; and (v) ensure that PII is being maintained and used only for the legally authorized purposes identified in the public notice(s). Organizations also: (i) implement technology to audit for the security, appropriate use, and loss of PII;	

	(ii) perform reviews to ensure physical security of documents containing PII; (iii) assess contractor compliance with privacy requirements; and (iv) ensure that corrective actions identified as part of the assessment process are tracked and monitored until audit findings are corrected. The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) coordinates monitoring and auditing efforts with information security officials and ensures that the results are provided to senior managers and oversight officials. Related controls: AR-6, AR-7, AU-1, AU-2, AU-3, AU-6, AU-12, CA-7, TR-1, UL-2. References: The Privacy Act of 1974, 5 U.S.C. § 552a; Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; Section 208, E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 05-08, 06-16, 07-16; OMB Circular A-130.	
	Implementation: (a) Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001, Program Managers and System Managers complete all Privacy Compliance Documentation set forth in applicable requirements (e.g., statutes regulations, Executive Orders, and policies issued by the Chief Privacy Officer),... [w]henever a DHS 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, the relevant manager completes a PTA in accordance with Privacy Office guidance and submits it to the Component Privacy Officer or PPOC. The Component Privacy Officer or PPOC reviews the proposed PTA in consultation with counsel for the Component and submits it, together with a recommendation as to whether a PIA is necessary, to the Chief Privacy Officer. The Chief Privacy Officer schedules completed PTAs, PIAs, and SORNs for mandatory review as follows: at least every three years for PTAs and PIAs, and every two years for SORNs. (b) Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001, the Chief Privacy Officer determines whether a PIA is required, based on answers provided in the PTA and taking into consideration the Component Privacy Officer's or PPOC's recommendation. In addition, the Chief Privacy Officer may conduct a Privacy Compliance Review of the system or program. Responsible Entitles: (a) System/Program Owner (b) DHS Chief Privacy Officer	
	Implementation Status: Implemented	Note: INSERTPIA and INSERTSORN complete and on file with DHS PRIV.
2.7	Privacy Awareness and Training	PRIV-AR-5
	Control: Privacy Awareness and Training The organization: (a) Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures; (b) Administers basic privacy training Annually and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII Annual privacy awareness training must be completed in VLC; and (c) Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements Annual privacy awareness training must be completed in VLC.. Supplemental Guidance Through implementation of a privacy training and awareness strategy, the organization promotes a culture of privacy. Privacy training and awareness programs typically focus on broad topics, such as responsibilities under the Privacy Act of 1974 and E-Government Act of 2002 and the consequences of failing to carry out those responsibilities, how to identify new privacy risks, how to mitigate privacy risks, and how and when to report privacy incidents. Privacy training may also target data collection and use requirements identified in public notices, such as Privacy Impact Assessments (PIAs) or System of Records Notices (SORNs) for a program or information system. Specific training methods may include: (i) mandatory annual privacy awareness training; (ii) targeted, role-based training; (iii) internal privacy program websites; (iv) manuals, guides, and handbooks; (v) slide presentations; (vi) events (e.g., privacy awareness week, privacy clean-up day); (vii) posters and brochures; and (viii) email messages to all employees and contractors. Organizations update training based on changing statutory, regulatory, mission, and Organizations	

	program, business process, and information system requirements, or on the results of compliance monitoring and auditing. Where appropriate, organizations may provide privacy training as part of existing information security training. Related controls: AR-3, AT-2, AT-3, TR-1. References: The Privacy Act of 1974, 5 U.S.C. § 552a(e); Section 208, E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 07-16.	
	Implementation: (a) DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001 require Privacy Training: New DHS Headquarters Component employees (other than Federal Law Enforcement Training Center employees) receive in-class privacy training provided by the Chief Privacy Officer during their orientation and six months thereafter. All DHS employees and contractors complete annual online privacy training developed by the Chief Privacy Officer or by Component Privacy Officers or PPOCs in consultation with the Chief Privacy Officer. Employees who handle Sensitive PII receive additional, role-based privacy training, if required in addition to Department-wide privacy training, developed by System Managers or Program Managers in consultation with Component Privacy Officers or PPOCs and the Chief Privacy Officer. (b)(1) DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001 require new DHS Headquarters Component employees (other than Federal Law Enforcement Training Center employees) receive in-class privacy training provided by the Chief Privacy Officer during their orientation and six months thereafter. All DHS employees and contractors complete annual online privacy training developed by the Chief Privacy Officer or by Component Privacy Officers or PPOCs in consultation with the Chief Privacy Officer. (b)(2) DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001 require employees who handle Sensitive PII receive additional, role-based privacy training developed by System Managers or Program Managers in consultation with Component Privacy Officers or PPOCs and the Chief Privacy Officer. System/Program owners, in consultation with the Component Privacy Officer or PPOC and the Chief Privacy Officer, are responsible for developing and implementing privacy procedures and job-related privacy training to safeguard PII in program and system operations, if necessary in addition to existing Department-wide privacy training. The frequency of the role-based training is determined by the system/program owners. (c)(1) New DHS Headquarters Component employees (other than Federal Law Enforcement Training Center employees) receive in-class privacy training provided by the Chief Privacy Officer during their orientation and six months thereafter. All DHS employees and contractors must certify completion of annual online privacy training developed by the Chief Privacy Officer or by Component Privacy Officers or PPOCs in consultation with the Chief Privacy Officer. (c)(2) Employees who handle Sensitive PII receive additional, role-based privacy training developed by System Managers or Program Managers in consultation with Component Privacy Officers or PPOCs and the Chief Privacy Officer. Responsible Entitles: (a) DHS Chief Privacy Officer (b)(1) DHS Chief Privacy Officer (b)(2) System/Program Owner (c)(1) DHS Chief Privacy Officer (c)(2) System/Program Owner	
	Implementation Status: Implemented	Note: INSERTPIA and INSERTSORN complete and on file with DHS PRIV.
2.8	Privacy Reporting	PRIV-AR-6
	Control: Privacy Reporting The organization develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance. Supplemental Guidance Through internal and external privacy reporting, organizations promote accountability and transparency in organizational privacy operations. Reporting also helps organizations to determine progress in meeting privacy compliance requirements and privacy controls, compare performance across the federal government, identify vulnerabilities and gaps in policy and implementation, and identify success models. Types of privacy reports include: (i) annual Senior Agency Official for Privacy (SAOP) reports to OMB; (ii) reports to Congress required by the Implementing Regulations of the 9/11 Commission Act; and (iii) other public reports required by	

	specific statutory mandates or internal policies of organizations. The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) consults with legal counsel, where appropriate, to ensure that organizations meet all applicable privacy reporting requirements. Related control: None. References: The Privacy Act of 1974, 5 U.S.C. § 552a; Section 208, E-Government Act of 2002 (P.L. 107-347); Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; Section 803, 9/11 Commission Act, 42 U.S.C. § 2000ee-1; Section 804, 9/11 Commission Act, 42 U.S.C. § 2000ee-3; Section 522, Consolidated Appropriations Act of 2005 (P.L. 108-447); OMB Memoranda 03-22; OMB Circular A-130.	
	Implementation: DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001 require the DHS Chief Privacy Officer to ensure that the Department meets all reporting requirements mandated by Congress or the Office of Management and Budget (OMB) regarding DHS activities that involve PII or otherwise impact privacy. All DHS reports are published on the public-facing website, www.dhs.gov/privacy and include the DHS Privacy Office Annual Report to Congress, the Data Mining Report, and reports required by the Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007. Responsible Entitles: DHS Chief Privacy Officer	
	Implementation Status: Implemented	Note: INSERTPIA and INSERTSORN complete and on file with DHS PRIV.
2.9	Privacy-Enhanced System Design and Development	PRIV-AR-7
	Control: Privacy-Enhanced System Design and Development The organization designs information systems to support privacy by automating privacy controls. Supplemental Guidance To the extent feasible, when designing organizational information systems, organizations employ technologies and system capabilities that automate privacy controls on the collection, use, retention, and disclosure of personally identifiable information (PII). By building privacy controls into system design and development, organizations mitigate privacy risks to PII, thereby reducing the likelihood of information system breaches and other privacy-related incidents. Organizations also conduct periodic reviews of systems to determine the need for updates to maintain compliance with the Privacy Act and the organization's privacy policy. Regardless of whether automated privacy controls are employed, organizations regularly monitor information system use and sharing of PII to ensure that the use/sharing is consistent with the authorized purposes identified in the Privacy Act and/or in the public notice of organizations, or in a manner compatible with those purposes. Related controls: AC-6, AR-4, AR-5, DM-2, TR-1. References: The Privacy Act of 1974, 5 U.S.C. § 552a(e)(10); Sections 208(b) and(c), E-Government Act of 2002 (P.L. 107-347); OMB Memorandum 03-22.	
	Implementation: Per "DHS Sensitive Systems" Policy Directive 4300A, subsection 3.14.2.g, the PTA process shall be used to ensure that DHS designs information systems to support privacy by automating privacy controls, to the greatest extent feasible. Responsible Entitles: DHS Chief Privacy Officer	
	Implementation Status: Implemented	Note: INSERTPIA and INSERTSORN complete and on file with DHS PRIV.
2.10	Accounting of Disclosures	PRIV-AR-8
	Control: Accounting of Disclosures The organization: (a) Keeps an accurate accounting of disclosures of information held in each system of records under its control, including: (1) Date, nature, and purpose of each disclosure of a record; and	

	(2) Name and address of the person or agency to which the disclosure was made; (b) Retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and (c) Makes the accounting of disclosures available to the person named in the record upon request. Supplemental Guidance The Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) periodically consults with managers of organization systems of record to ensure that the required accountings of disclosures of records are being properly maintained and provided to persons named in those records consistent with the dictates of the Privacy Act. Organizations are not required to keep an accounting of disclosures when the disclosures are made to individuals with a need to know, are made pursuant to the Freedom of Information Act, or are made to a law enforcement agency pursuant to 5 U.S.C. § 552a(c)(3). Heads of agencies can promulgate rules to exempt certain systems of records from the requirement to provide the accounting of disclosures to individuals. Related control: IP-2. References: The Privacy Act of 1974, 5 U.S.C. § 552a (c)(1), (c)(3), (j), (k).	
	Implementation: All DHS systems/programs: (a) Keep an accurate accounting of disclosures of information held in each system of records under its control, including: (1) Date, nature, and purpose of each disclosure of a record; and (2) Name and address of the person or agency to which the disclosure was made; retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and makes the accounting of disclosures available to the person named in the record upon request. All DHS systems/programs: (a) Keep an accurate accounting of disclosures of information held in each system of records under its control, including: (1) Date, nature, and purpose of each disclosure of a record; and (2) Name and address of the person or agency to which the disclosure was made; retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and makes the accounting of disclosures available to the person named in the record upon request. Unless exempted by the Privacy Act, all DHS systems/programs: (a) Keep an accurate accounting of disclosures of information held in each system of records under its control, including: (1) Date, nature, and purpose of each disclosure of a record; and (2) Name and address of the person or agency to which the disclosure was made; retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and makes the accounting of disclosures available to the person named in the record upon request. Responsible Entitles: (a) System/Program Owner (b) System/Program Owner (c) System/Program Owner	
	Implementation Status: Implemented	Note: INSERTPIA and INSERTSORN complete and on file with DHS PRIV.
2.11	Data Quality	PRIV-DI-1
	Control: Data Quality The organization: (a) Confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information; (b) Collects PII directly from the individual to the greatest extent practicable; (c) Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems The systems require users to update incorrect records as they find them; and (d) Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information. Supplemental Guidance Organizations take reasonable steps to confirm the accuracy and relevance of PII. Such steps may include, for example, editing and validating addresses as they are collected or entered into information systems using automated address verification look-up application programming interfaces (API). The types of measures taken to protect data quality are based on the nature and context of the PII, how it is to be used, and how it was obtained. Measures taken to validate the accuracy of PII that is used to make	

	determinations about the rights, benefits, or privileges of individuals under federal programs may be more comprehensive than those used to validate less sensitive PII. Additional steps may be necessary to validate PII that is obtained from sources other than individuals or the authorized representatives of individuals. When PII is of a sufficiently sensitive nature (e.g., when it is used for annual reconfirmation of a taxpayer's income for a recurring benefit), organizations incorporate mechanisms into information systems and develop corresponding procedures for how frequently, and by what method, the information is to be updated. Related controls: AP-2, DI-2, DM-1, IP-3, SI-10. References: The Privacy Act of 1974, 5 U.S.C. § 552a (c) and (e); Treasury and General Government Appropriations Act for Fiscal Year 2001 (P.L. 106-554), app C § 515, 114 Stat. 2763A-153-4; Paperwork Reduction Act, 44 U.S.C. § 3501; OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies (October 2001); OMB Memorandum 07-16.	
	Implementation: (a) PIA section 2.4 requires System/Program owners to explain how the project checks the accuracy of the information that the system/program uses or maintains. Describe the process used for checking accuracy. If a commercial data aggregator is involved describe the levels of accuracy required by the contract. Sometimes information is assumed to be accurate, or in R&D, inaccurate information may not have an impact on the individual or the project. If the project does not check for accuracy, please explain why. Describe any technical solutions, policies, or procedures focused on improving data accuracy and integrity of the project. (b) PIA section 2.5 Privacy Impact Analysis: Related to Characterization of the Information. Given the specific data elements collected, discuss the privacy risks identified and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included. System/Program owners must consider the principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual? (c) PIA section 2.4 requires System/Program owners explain how the project checks the accuracy of the information. Describe the process used for checking accuracy. If a commercial data aggregator is involved describe the levels of accuracy required by the contract. Sometimes information is assumed to be accurate, or in R&D, inaccurate information may not have an impact on the individual or the project. If the project does not check for accuracy, please explain why. Describe any technical solutions, policies, or procedures focused on improving data accuracy and integrity of the project. DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001 and 4300A "Sensitive Systems Policy," subsection 3.14.2 require that whenever a DHS 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, the relevant manager completes a PTA in accordance with Privacy Office guidance and submits it to the Component Privacy Officer or PPOC. Component Privacy Officer or PPOC reviews the proposed PTA in consultation with counsel for the Component and submits it, together with a recommendation as to whether a PIA is necessary, to the Chief Privacy Officer. PTAs expire after three years. (d) DHS issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information, including the DHS "Information Sharing Access Agreements Guidebook," Privacy Policy Guidance Memorandum 2007-01, "Regarding Collection Use, Retention, and Dissemination of Information on Non-U.S. Persons" (as amended January 7, 2009), and the DHS INSERTPIA and INSERTSORNguidance. Responsible Entitles: (a) System/Program Owner (b) System/Program Owner (c) System/Program Owner (d) DHS Chief Privacy Officer	
	Implementation Status: Implemented	Note: INSERTPIA and INSERTSORN complete and on file with DHS PRIV.
2.12	Data Integrity and Data Integrity Board	PRIV-DI-2
	Control: Data Integrity and Data Integrity Board The organization: (a) Documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls; and,	

	(b) Establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements123 and to ensure that those agreements comply with the computer matching provisions of the Privacy Act. Supplemental Guidance Organizations conducting or participating in Computer Matching Agreements with other organizations regarding applicants for and recipients of financial assistance or payments under federal benefit programs or regarding certain computerized comparisons involving federal personnel or payroll records establish a Data Integrity Board to oversee and coordinate their implementation of such matching agreements. In many organizations, the Data Integrity Board is led by the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO). The Data Integrity Board ensures that controls are in place to maintain both the quality and the integrity of data shared under Computer Matching Agreements. Related controls: AC-1, AC-3, AC-4, AC-6, AC-17, AC-22, AU-2, AU-3, AU-6, AU-10, AU-11, DI-1, SC-8, SC-28, UL-2. References: The Privacy Act of 1974, 5 U.S.C. §§ 552a (a)(8)(A), (o), (p), (u); OMB Circular A-130, Appendix I.	
	Implementation: (a) PIA section 1.3 requires System/Program owners provide the date that the Authority to Operate (ATO) was granted or the date it is expected to be awarded. An operational system must comply with DHS Management Directive 4300A, which includes all NIST 800-53 security and privacy controls. Note that all systems containing PII are categorized at a minimum as "moderate" under Federal Information Processing Standards Publication 199. If the project does not trigger the C&A requirement, System/Program owners must state that along with an explanation. (b) DHS MD 262-01, "Computer Matching Agreements and the Data Integrity Board," effectuates a Data Integrity Board (DIB) for DHS and provides policies for engaging in and approving Computer Matching Agreements (CMAs) that fall under the Privacy Act of 1974, as amended (5 U.S.C. § 552a). Responsible Entitles: (a) System/Program Owner (b) DHS Chief Privacy Officer	
	Implementation Status: Implemented	Note: INSERTPIA and INSERTSORN complete and on file with DHS PRIV.
2.13	Minimization of Personally Identifiable Information	PRIV-DM-1
	Control: Minimization of Personally Identifiable Information The organization: (a) identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection; (b) limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and, (c) conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings The systems require users to update incorrect records as they find them to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose. Supplemental Guidance Organizations take appropriate steps to ensure that the collection of PII is consistent with a purpose authorized by law or regulation. The minimum set of PII elements required to support a specific organization business process may be a subset of the PII the organization is authorized to collect. Program officials consult with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and legal counsel to identify the minimum PII elements required by the information system or activity to accomplish the legally authorized purpose. Organizations can further reduce their privacy and security risks by also reducing their inventory of PII, where appropriate. OMB Memorandum 07-16 requires organizations to conduct both an initial review and subsequent reviews of their holdings of all PII and ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely, and complete. Organizations are also directed by OMB to reduce their holdings to the minimum necessary for the proper performance of a documented organizational business purpose. OMB Memorandum 07-16 requires organizations to develop and publicize, either through a notice in the Federal	

	Register or on their websites, a schedule for periodic reviews of their holdings to supplement the initial review. Organizations coordinate with their federal records officers to ensure that reductions in organizational holdings of PII are consistent with NARA retention schedules. By performing periodic evaluations, organizations reduce risk, ensure that they are collecting only the data specified in the notice, and ensure that the data collected is still relevant and necessary for the purpose(s) specified in the notice. Related controls: AP-1, AP-2, AR-4, IP-1, SE-1, SI-12, TR-1. References: The Privacy Act of 1974, 5 U.S.C. §552a (e); Section 208(b), E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 07-16.	
	Implementation: (a) PIA section 2.5 Privacy Impact Analysis: Related to Characterization of the Information. Given the specific data elements collected, discuss the privacy risks identified and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included. System/Program owners must consider the principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program? (b) PIA section 2.5 Privacy Impact Analysis: Related to Characterization of the Information. Given the specific data elements collected, discuss the privacy risks identified and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included. System/Program owners must consider the principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program? (c) DHS MD 047-01 "Privacy Policy Compliance" and corresponding Instruction 047-01-001, and PTA process generally, requires whenever a DHS 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, the relevant manager completes a PTA in accordance with Privacy Office guidance and submits it to the Component Privacy Officer or PPOC. The Component Privacy Officer or PPOC reviews the proposed PTA in consultation with counsel for the Component and submits it, together with a recommendation as to whether a PIA is necessary, to the Chief Privacy Officer. The Chief Privacy Officer determines whether a PIA is required, based on answers provided in the PTA and taking into consideration the Component Privacy Officer's or PPOC's recommendation. Responsible Entitles: (a) System/Program Owner (b) System/Program Owner (c) DHS Chief Privacy Officer	
	Implementation Status: Implemented	Note: INSERTPIA and INSERTSORN complete and on file with DHS PRIV.
2.14	Data Retention and Disposal	PRIV-DM-2
	Control: Data Retention and Disposal The organization: (a) retains each collection of personally identifiable information (PII) for Varies by system according to the System of Records Notice and NARA retention schedule. Ranges up to 75 years for law enforcement and immigration records, or as little as a year to fulfill the purpose(s) identified in the notice or as required by law; (b) disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and, (c) uses Utilization of a wipe disk, approved shredder to ensure secure deletion or destruction of PII (including originals, copies, and archived records). Supplemental Guidance NARA provides retention schedules that govern the disposition of federal records. Program officials coordinate with records officers and with NARA to identify appropriate retention periods and disposal methods. NARA may require organizations to retain PII longer than is operationally needed. In those situations, organizations describe such requirements in the notice. Methods of storage include, for example, electronic, optical media, or paper. Examples of ways organizations may reduce holdings include reducing the types of PII held (e.g., delete Social Security numbers if	

	their use is no longer needed) or shortening the retention period for PII that is maintained if it is no longer necessary to keep PII for long periods of time (this effort is undertaken in consultation with an organization's records officer to receive NARA approval). In both examples, organizations provide notice (e.g., an updated System of Records Notice) to inform the public of any changes in holdings of PII. Certain read-only archiving techniques, such as DVDs, CDs, microfilm, or microfiche, may not permit the removal of individual records without the destruction of the entire database contained on such media. Related controls: AR-4, AU-11, DM-1, MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SI-12, TR-1. References: The Privacy Act of 1974, 5 U.S.C. § 552a (e)(1), (c)(2); Section 208 (e), E-Government Act of 2002 (P.L. 107-347); 44 U.S.C. Chapters 29, 31, 33; OMB Memorandum 07-16; OMB Circular A-130; NIST Special Publication 800-88.	
	Implementation: (a) PIA section 5.0, Data Retention by the Project, requires system/program owners to explain the nexus between the original purpose for the collection and this retention period. The minimum amount of information should be maintained for the minimum amount of time in order to support the project. Retention schedules will vary based on the NARA schedule applicable for the system/program. (b) PIA section 1.5 requires the project manager, in consultation with counsel and the component records management officer, must develop a records retention schedule for the records contained in the project that considers the minimum amount of time necessary to retain information while meeting the needs of the project. After the project manager and component records management officer finalize the schedule based on the needs of the project, it is proposed to NARA for official approval. Consult with your records management office for assistance with this question if necessary. If a NARA-approved schedule does not exist, explain what stage the project is in developing and submitting a records retention schedule. (c) Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001, System Owners and Program Managers are responsible for establishing administrative, technical, and physical controls for storing and safeguarding PII consistent with DHS privacy, security, and records management requirements to ensure the protection of PII from unauthorized access, disclosure, or destruction. See also the procedures detailed in the DHS Handbook for Safeguarding Sensitive Personally Identifiable Information. Responsible Entitles: (a) System/Program Owner (b) System/Program Owner (c) System/Program Owner	
	Implementation Status: Implemented	Note: INSERTPIA and INSERTSORN complete and on file with DHS PRIV.
2.15	Minimization of PII Used in Testing, Training, and Research	PRIV-DM-3
	Control: Minimization of PII Used in Testing, Training, and Research The organization: (a) develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and, (b) implements controls to protect PII used for testing, training, and research. Supplemental Guidance: Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. The use of PII in testing, research, and training increases risk of unauthorized disclosure or misuse of the information. If PII must be used, organizations take measures to minimize any associated risks and to authorize the use of and limit the amount of PII for these purposes. Organizations consult with the SAOP/CPO and legal counsel to ensure that the use of PII in testing, training, and research is compatible with the original purpose for which it was collected. Related control: None. References: NIST Special Publication 800-122.	

	Implementation: (a) DHS MD 140-06 "Privacy Policy for Research Programs and Projects" establishes the DHS privacy policy for DHS privacy-sensitive research programs and projects. DHS adopts the Principles for Implementing Privacy Protections in DHS Research Projects first enunciated in the 2008 Report to Congress on Data Mining: Technology and Policy (December, 2008) as privacy policy for all DHS privacy-sensitive research. The Chief Privacy Officer determines privacy policy and standards for DHS privacy-sensitive research programs and projects consistent with the Principles for Implementing Privacy Protections in DHS Research Projects; provides privacy guidance and training to DHS personnel involved in privacy-sensitive research; and provides support on privacy-related matters to DHS Components' research efforts. Component heads work with the Chief Privacy Officer to ensure that privacy-sensitive research programs and projects follow DHS privacy policy and standards, thereby enhancing the overall consistency of privacy protections across DHS research, and develop an implementation plan for privacy-sensitive research. (b) DHS MD 140-06-001 "Privacy Policy for Research Programs and Projects Instruction," requires System and Program owners to complete a PTA in accordance with the Component privacy implementation plan. DHS Privacy Office staff and the Component Privacy Officer or PPOC review each PTA to determine how best to apply the DHS Fair Information Practice Principles to each privacy-sensitive program or project. The DHS Privacy Office assists the Component Privacy Officer or PPOC, as appropriate, in identifying privacy impacts to address in a privacy-sensitive program's or project's design and implementation, to ensure that privacy-sensitive research programs or projects sustain privacy protections relating to the collection, use, disclosure, retention, and destruction of PII pursuant to 6 U.S.C . § 142(a)(1). An appropriately cleared Component or external expert participates in the privacy assessment to explain scientific aspects of a proposed privacy-sensitive research program or project where a deeper understanding is needed to make decisions regarding the use of PII. Protections for data use in testing and training are found in Component policies regarding live data, some of which are currently in development. Responsible Entitles: (a) DHS Chief Privacy Officer (b) System/Program Owner	
	Implementation Status: Implemented	Note: INSERTPIA and INSERTSORN complete and on file with DHS PRIV.
2.16	Consent	PRIV-IP-1
	Control: Consent The organization: (a) Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection; (b) Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII; (c) Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and (d) Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII. Supplemental Guidance Consent is fundamental to the participation of individuals in the decision-making process regarding the collection and use of their PII and the use of technologies that may increase risk to personal privacy. To obtain consent, organizations provide individuals appropriate notice of the purposes of the PII collection or technology use and a means for individuals to consent to the activity. Organizations tailor the public notice and consent mechanisms to meet operational needs. Organizations achieve awareness and consent, for example, through updated public notices. Organizations may obtain consent through opt-in, opt-out, or implied consent. Opt-in consent is the preferred method, but it is not always feasible. Opt-in requires that individuals take affirmative action to allow organizations to collect or use PII. For example, opt-in consent may require an individual to click a radio button on a website, or sign a document providing consent. In contrast, opt-out requires individuals to take action to prevent the new or continued collection or use of such PII. For example, the Federal Trade Commission's Do-Not-Call Registry allows individuals to opt-out of receiving unsolicited telemarketing calls by requesting to be added to a list. Implied consent is the least preferred method and should be used in limited circumstances. Implied consent occurs where individuals' behavior or failure to object indicates agreement with the collection or use of PII (e.g., by entering and remaining in a building where notice has been posted that security cameras are in use, the individual implies consent to the video recording). Depending upon the nature of the program or information system, it may be appropriate to allow individuals to limit the types of PII they provide and subsequent uses of that PII. Organizational consent mechanisms include a discussion of the consequences to individuals of failure to provide PII. Consequences can vary from organization to organization.	

	Related controls: AC-2, AP-1, TR-1, TR-2. References: The Privacy Act of 1974, 5 U.S.C. § 552a (b), (e)(3); Section 208(c), E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 10-22.	
	Implementation: (a) Section 4.2 of the PIA requires System/Program owners to provide the opportunities available for individuals to consent to uses, decline or provide information, or opt out of the project. This question is directed at whether the individual from or about whom information is collected can decline to provide the information and if so, whether the consequences of providing the information are included in the notice. Additionally, System/Program owners must state whether an individual may provide consent for specific uses or whether consent is given to cover all uses (current or potential) of his/her information. If specific consent is permitted or required, how does the individual consent to each use? If notice is provided to explain how an individual may exercise the right to consent to particular uses or decline to provide information describe the process. If this is not an option, explain why not. In some cases, declining to provide information simply means the individual chooses not to participate in the project. (b) DHS provides written or oral notice before collecting information from individuals. That notice may include a posted privacy policy, a Privacy Act statement on forms, a PIA, or a SORN published in the Federal Register. Privacy Act Statements at the time of information collection, if applicable, provide individuals an opportunity to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII. For certain law enforcement projects, notice may not be appropriate – Section 4.0 of the PIA requires System/Program owners to explain how providing direct notice to the individual at the time of collection would undermine the law enforcement mission. (c) Section 4.2 of the PIA requires System/Program owners to provide the opportunities available for individuals to consent to uses, decline or provide information, or opt out of the project. This question is directed at whether the individual from or about whom information is collected can decline to provide the information and if so, whether the consequences of providing the information are included in the notice. Additionally, System/Program owners must state whether an individual may provide consent for specific uses or whether consent is given to cover all uses (current or potential) of his/her information. If specific consent is permitted or required, how does the individual consent to each use? If notice is provided to explain how an individual may exercise the right to consent to particular uses or decline to provide information describe the process. If this is not an option, explain why not. In some cases, declining to provide information simply means the individual chooses not to participate in the project. (d) Section 4.3 of the PIA requires System/Program owners to discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent. Consider the following FIPPs below to assist in providing a response: Principle of Transparency: Has sufficient notice been provided to the individual? Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice? Principle of Individual Participation: Has the program provided notice to the individual of how the program provides for redress including access and correction, including other purposes of notice such as types of information and controls over security, retention, disposal, etc.? Responsible Entitles: (a) System/Program Owner (b) System/Program Owner (c) System/Program Owner (d) System/Program Owner	
	Implementation Status: Implemented	Note: INSERTPIA and INSERTSORN complete and on file with DHS PRIV.
2.17	Individual Access	PRIV-IP-2
	Control: Individual Access The organization: (a) Provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records; (b) Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records; (c) Publishes access procedures in System of Records Notices (SORNs); and (d) Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.	

	Supplemental Guidance Access affords individuals the ability to review PII about them held within organizational systems of records. Access includes timely, simplified, and inexpensive access to data. Organizational processes for allowing access to records may differ based on resources, legal requirements, or other factors. The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) is responsible for the content of Privacy Act regulations and record request processing, in consultation with legal counsel. Access to certain types of records may not be appropriate, however, and heads of agencies may promulgate rules exempting particular systems from the access provision of the Privacy Act. In addition, individuals are not entitled to access to information compiled in reasonable anticipation of a civil action or proceeding. Related controls: AR-8, IP-3, TR-1, TR-2. References: The Privacy Act of 1974, 5 U.S.C. §§ 552a (c)(3), (d)(5), (e) (4); (j), (k), (t); OMB Circular A-130.	
	Implementation: (a) PIA Section 7.1 requires System/Program owners to describe the procedures to allow individuals to access their information. System/Program owners must describe any procedures or regulations their component has in place that allow access to information collected by the system or project and/or to an accounting of disclosures of that information. Generally speaking, these procedures should include the Department's FOIA/Privacy Act practices. If the Privacy Act does not apply, state why this is the case. If additional mechanisms exist, include those in this section. For example, if a component has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the Department's procedures. If the system is exempt from the access provisions of the Privacy Act, explain the basis for the exemption and cite the Final Rule published in the Code of Federal Regulations (CFR) that explains this exemption. If the project is not a Privacy Act system, explain what procedures and/or regulations are in place that cover an individual gaining access to his/her own information. (b) Rules and regulations governing how individuals may request access to records maintained in a DHS Privacy Act system of records are available in individual DHS System of Record Notices published in the Federal Register. Final Rules exempting systems from certain provisions of the Privacy Act are available at 6 CFR Part 5. (c) All DHS SORNs must contain sections describing the notification procedures, record access procedures, and contesting record procedures. Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Chief Privacy Officer. Individuals seeking records about themselves from a system of records must conform to the Privacy Act regulations set forth in 6 CFR Part 5. (d) See 6 CFR Part 5, and Privacy Policy Guidance Memorandum 2011-01, "Privacy Act Amendment Requests" (February 11, 2011), which sets out the Chief Privacy Officer's guidance for processing Privacy Act Amendment requests. Responsible Entitles: (a) System/Program Owner (b) DHS Chief Privacy Officer (c) System/Program Owner (d) DHS Chief Privacy Officer	
	Implementation Status: Implemented	Note: INSERTPIA and INSERTSORN complete and on file with DHS PRIV.
2.18	Redress	PRIV-IP-3
	Control: Redress The organization: (a) Provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate; and, (b) Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended. Supplemental Guidance Redress supports the ability of individuals to ensure the accuracy of PII held by organizations. Effective redress processes demonstrate organizational commitment to data quality especially in those business functions where inaccurate data may result in inappropriate decisions or denial of benefits and services to individuals. Organizations use discretion in determining if records are to	

	be corrected or amended, based on the scope of redress requests, the changes sought, and the impact of the changes. Individuals may appeal an adverse decision and have incorrect information amended, where appropriate. To provide effective redress, organizations: (i) provide effective notice of the existence of a PII collection; (ii) provide plain language explanations of the processes and mechanisms for requesting access to records; (iii) establish criteria for submitting requests for correction or amendment; (iv) implement resources to analyze and adjudicate requests; (v) implement means of correcting or amending data collections; and (vi) review any decisions that may have been the result of inaccurate information. Organizational redress processes provide responses to individuals of decisions to deny requests for correction or amendment, including the reasons for those decisions, a means to record individual objections to the organizational decisions, and a means of requesting organizational reviews of the initial determinations. Where PII is corrected or amended, organizations take steps to ensure that all authorized recipients of that PII are informed of the corrected or amended information. In instances where redress involves information obtained from other organizations, redress processes include coordination with organizations that originally collected the information. Related controls: IP-2, TR-1, TR-2, UL-2. References: The Privacy Act of 1974, 5 U.S.C. § 552a (d), (c)(4); OMB Circular A-130.	
	Implementation: (a) DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001 and the Privacy Policy Guidance Memorandum 2011-01, "Privacy Act Amendment Requests" (February 11, 2011) sets forth DHS policy on identifying, processing, tracking, and reporting on requests for amendment of records submitted to DHS under the Privacy Act of 1974, as amended (Amendment Requests). DHS Component Privacy Officers and FOIA Officers shall have robust and documented procedures for identifying, processing, tracking, and reporting on Amendment Requests. Records found in a Privacy Act System of Records and not otherwise exempted are subject to the right to amend. This right is available to individuals whether the request is processed by Component Privacy Officers or FOIA Officers. Components should determine, as part of their documented process, whether the Component Privacy Officer or FOIA Officer will be responsible for identifying, processing, tracking, and reporting Amendment Requests understanding that significant collaboration between the two Officers shall occur. (b) DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001 and the Privacy Policy Guidance Memorandum 2011-01, "Privacy Act Amendment Requests" (February 11, 2011) sets forth DHS policy on identifying, processing, tracking, and reporting on requests for amendment of records submitted to DHS under the Privacy Act of 1974, as amended (Amendment Requests). After identifying from the requester which records in a given non-exempt Privacy Act System(s) of Records the requester would like for the Department to amend, the Component Privacy Officer or FOIA Officer should forward the request to the appropriate system manager. The system manager should then confirm that the requester is a subject of a record in the specified Privacy Act System(s) of Records. The system manager, in consultation with the Component Privacy Officer or FOIA Officer as well as Counsel, shall make the determination as to whether to amend the record(s) and then shall notify the requester in writing after the initial determination. If the record will be amended, a notification should be sent to system manager(s) informing them of the update and requiring the change be made. If an initial determination is made to deny amendment, the Component Privacy Officer or FOIA Officer will notify the requester of this information and how to appeal the denial, should the requestor choose to do so. Responsible Entitles: (a) DHS Chief Privacy Officer (b) System/Program Owner	
	Implementation Status: Implemented	Note: INSERTPIA and INSERTSORN complete and on file with DHS PRIV.
2.19	Complaint Management	PRIV-IP-4
	Control: Complaint Management The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the	

	organizational privacy practices. Supplemental Guidance Complaints, concerns, and questions from individuals can serve as a valuable source of external input that ultimately improves operational models, uses of technology, data collection practices, and privacy and security safeguards. Organizations provide complaint mechanisms that are readily accessible by the public, include all information necessary for successfully filing complaints (including contact information for the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) or other official designated to receive complaints), and are easy to use. Organizational complaint management processes include tracking mechanisms to ensure that all complaints received are reviewed and appropriately addressed in a timely manner. Related controls: AR-6, IP-3. References: OMB Circular A-130; OMB Memoranda 07-16, 08-09.	
	Implementation: DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001 requires that the Chief Privacy Officer processes privacy complaints from organizations and individuals regarding Department activities and ensuring that redress is provided, where appropriate. The Chief Privacy Officer collaborates with Component Privacy Officers to review privacy complaints received throughout DHS, and to provide redress as appropriate. Under the terms of a March 2008 Memorandum of Understanding between the Chief Privacy Officer and the DHS Inspector General, OIG has the opportunity to decide whether to conduct investigations of allegations of criminal misconduct, systemic violations, serious management problems, and allegations of non-criminal misconduct by employees at the GS-15 level or higher and all political and Schedule C employees, and, where it declines to do so, refers the matter to the Privacy Office for review and resolution. The Chief Privacy Officer also reviews and responds to traveler complaints related to privacy received through the DHS Traveler Redress Inquiry Program (DHS TRIP). Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001, Components review component-specific complaints. Responsible Entitles: DHS Chief Privacy Officer	
	Implementation Status: Implemented	Note: INSERTPIA and INSERTSORN complete and on file with DHS PRIV.
2.20	Inventory of Personally Identifiable Information	PRIV-SE-1
	Control: Inventory of Personally Identifiable Information The organization: (a) Establishes, maintains, and updates Quarterly an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); and (b) Provides each update of the PII inventory to the CIO or information security official Annually to support the establishment of information security requirements for all new or modified information systems containing PII. Supplemental Guidance The PII inventory enables organizations to implement effective administrative, technical, and physical security policies and procedures to protect PII consistent with Appendix F, and to mitigate risks of PII exposure. As one method of gathering information for their PII inventories, organizations may extract the following information elements from Privacy Impact Assessments (PIA) for information systems containing PII: (i) the name and acronym for each system identified; (ii) the types of PII contained in that system; (iii) classification of level of sensitivity of all types of PII, as combined in that information system; and (iv) classification of level of potential risk of substantial harm, embarrassment, inconvenience, or unfairness to affected individuals, as well as the financial or reputational risks to organizations, if PII is exposed. Organizations take due care in updating the inventories by identifying linkable data that could create PII. Related controls: AR-1, AR-4, AR-5, AT-1, DM-1, PM-5, UL-3. References: The Privacy Act of 1974, 5 U.S.C. § 552a (e) (10); Section 208(b)(2), E-Government Act of 2002 (P.L. 107-347); OMB Memorandum 03-22; OMB Circular A-130, Appendix I; FIPS Publication 199; NIST Special Publications 800-37, 800-122.	

	Implementation: (a) DHS "Sensitive Systems" Policy Directive 4300A, subsection 3.14.2.f, requires that the PTA process is used to maintain a current inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII. (b) DHS "Sensitive Systems" Policy Directive 4300A, subsection 3.14.2.f, requires the PTA process is used to maintain a current inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII. The DHS Privacy Office provides a component breakdown of the PII inventory and compliance status to the DHS CISO on a quarterly and annual basis as part of the FISMA reporting requirements. Responsible Entitles: (a) DHS Chief Privacy Officer (b) DHS Chief Privacy Officer	
	Implementation Status: Implemented	Note: INSERTPIA and INSERTSORN complete and on file with DHS PRIV.
2.21	Privacy Incident Response	PRIV-SE-2
	Control: Privacy Incident Response The organization: In contrast to the Incident Response (IR) family in Appendix F, which concerns a broader range of incidents affecting information security, this control uses the term Privacy Incident to describe only those incidents that relate to personally identifiable information (PII). The organization Privacy Incident Response Plan is developed under the leadership of the SAOP/CPO. The plan includes: (i) the establishment of a cross-functional Privacy Incident Response Team that reviews, approves, and participates in the execution of the Privacy Incident Response Plan; (ii) a process to determine whether notice to oversight organizations or affected individuals is appropriate and to provide that notice accordingly; (iii) a privacy risk assessment process to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and, where appropriate, to take steps to mitigate any such risks; (iv) internal procedures to ensure prompt reporting by employees and contractors of any privacy incident to information security officials and the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO), consistent with organizational incident management structures; and (v) internal procedures for reporting noncompliance with organizational privacy policy by employees or contractors to appropriate management or oversight officials. Some organizations may be required by law or policy to provide notice to oversight organizations in the event of a breach. Organizations may also choose to integrate Privacy Incident Response Plans with Security Incident Response Plans, or keep the plans separate. Related controls: AR-1, AR-4, AR-5, AR-6, AU-1 through 14, IR-1 through IR-8, RA-1. Control Enhancements: None. References: The Privacy Act of 1974, 5 U.S.C. § 552a (e), (i)(1), and (m); Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; OMB Memoranda 06-19, 07-16; NIST Special Publication 800-37.	
	Implementation: (a) The "DHS Privacy Incident Handling Guidance" (January 2012), informs all Department personnel of their obligation to protect PII, it also establishes procedures delineating how they must respond to the potential loss or compromise of PII. (b) The "DHS Privacy Incident Handling Guidance" (January 2012), informs all Department personnel of their obligation to protect PII, it also establishes procedures delineating how they must respond to the potential loss or compromise of PII. Responsible Entitles: (a) DHS Chief Privacy Officer (b) DHS Chief Privacy Officer	
	Implementation Status: Implemented	Note: INSERTPIA and INSERTSORN complete and on file with DHS PRIV.

2.22	Privacy Notice	PRIV-TR-1

Control: Privacy Notice

The organization:

(a) Provides effective notice to the public and to individuals regarding:

(i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII);
(ii) authority for collecting PII;
(iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and
(iv) the ability to access and have PII amended or corrected if necessary;

(b) Describes:

(i) the PII the organization collects and the purpose(s) for which it collects that information;
(ii) how the organization uses PII internally;
(iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing;
(iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent;
(v) how individuals may obtain access to PII; and
(vi) how the PII will be protected; and

(c) Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.

Supplemental Guidance

Effective notice, by virtue of its clarity, readability, and comprehensiveness, enables individuals to understand how an organization uses PII generally and, where appropriate, to make an informed decision prior to providing PII to an organization. Effective notice also demonstrates the privacy considerations that the organization has addressed in implementing its information practices. The organization may provide general public notice through a variety of means, as required by law or policy, including System of Records Notices (SORNs), Privacy Impact Assessments (PIAs), or in a website privacy policy. As required by the Privacy Act, the organization also provides direct notice to individuals via Privacy Act Statements on the paper and electronic forms it uses to collect PII, or on separate forms that can be retained by the individuals.

The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) is responsible for the content of the organization's public notices, in consultation with legal counsel and relevant program managers. The public notice requirement in this control is satisfied by an organization's compliance with the public notice provisions of the Privacy Act, the E-Government Act's PIA requirement, with OMB guidance related to federal agency privacy notices, and, where applicable, with policy pertaining to participation in the Information Sharing Environment (ISE).124 Changing PII practice or policy without prior notice is disfavored and should only be undertaken in consultation with the SAOP/CPO and counsel.

Related controls: AP-1, AP-2, AR-1, AR-2, IP-1, IP-2, IP-3, UL-1, UL-2.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3), (e)(4); Section 208(b), E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 07-16, 10-22, 10-23; ISE Privacy Guidelines.

Implementation: (a) Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001, System/Program owners are responsible for providing effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary. System/Program owners may provide notice through PIAs, SORNs, public-facing websites, and Privacy Act Statements as appropriate.

(b) Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001, System/Program owners are responsible for describing (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for

	such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected. System/Program owners may provide notice through PIAs, SORNs, public-facing websites, and Privacy Act State+F4ments as appropriate. (c) DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001 require System/Program owners must revise their public notices to reflect changes in practice or policy that affect PII or changes in their activities that impact privacy, before or as soon as practicable after the change. The PTA process identifies when privacy compliance documentation and subsequent notices require an update. The Chief Privacy Officer schedules completed PTAs, PIAs, and SORNs for mandatory review as follows: at least every three years for PTAs and PIAs, and every two years for SORNs. The Chief Privacy Officer notifies the relevant Component Privacy Officer or PPOC that a PTA, PIA, and/or SORN review is required and begins the collaborative review process, which follows the process described in this Instruction for new PTAs, PIAs, and SORNs. Responsible Entitles: (a) System/Program Owner (b) System/Program Owner (c) System/Program Owner	
	Implementation Status: Implemented	Note: INSERTPIA and INSERTSORN complete and on file with DHS PRIV.
2.23	System of Records Notices and Privacy Act Statements	PRIV-TR-2
	Control: System of Records Notices and Privacy Act Statements The organization: (a) Publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PII); (b) Keeps SORNs current; and (c) Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected. Supplemental Guidance Organizations issue SORNs to provide the public notice regarding PII collected in a system of records, which the Privacy Act defines as "a group of any records under the control of any agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifier." SORNs explain how the information is used, retained, and may be corrected, and whether certain portions of the system are subject to Privacy Act exemptions for law enforcement or national security reasons. Privacy Act Statements provide notice of: (i) the authority of organizations to collect PII; (ii) whether providing PII is mandatory or optional; (iii) the principal purpose(s) for which the PII is to be used; (iv) the intended disclosures (routine uses) of the information; and (v) the consequences of not providing all or some portion of the information requested. When information is collected verbally, organizations read a Privacy Act Statement prior to initiating the collection of PII (for example, when conducting telephone interviews or surveys). Related control: DI-2. References: The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3); OMB Circular A-130.	
	Implementation: (a) DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001, require the Chief Privacy Officer, in consultation with the relevant Component Privacy Officer or PPOC and counsel for the Component, determines whether a particular collection of PII is a System of Records for Privacy Act purposes and whether to propose a rule that would exempt the system from certain aspects of the Privacy Act. If the system is a Privacy Act System of Records and it is not covered by an existing SORN, the Component Privacy Officer or PPOC, in consultation with counsel for the Component, prepares a SORN and, where appropriate, an NPRM describing proposed Privacy Act exemptions for the System of Records and, after public comment, a Final Rule, in accordance with guidance issued by the Chief Privacy Officer. The Chief Privacy Officer reviews and provides final approval for all SORNs, NPRMs, and Final Rules. (b) System/Program owners review SORNs biennially, as required by OMB Circular A-130. (c) Consistent with guidance issued by the Chief Privacy Officer, DHS Directive 047-01 "Privacy Policy and Compliance" and	

	Instruction 047-01-001 require Program Managers and System Managers submit drafts of all Privacy Act Statements to the Chief Privacy Officer, or to the relevant Component Privacy Officer or PPOC, for review and final approval. Privacy Act Statements are included in all documents, whether in paper or electronic form, that the Department uses to collect PII from individuals to be maintained in a Privacy Act System of Records. Responsible Entitles: (a) System/Program Owner (b) System/Program Owner (c) System/Program Owner	
	Implementation Status: Implemented	Note: INSERTPIA and INSERTSORN complete and on file with DHS PRIV.
2.24	Dissemination of Privacy Program Information	PRIV-TR-3
	Control: Dissemination of Privacy Program Information The organization: (a) Ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO); and (b) Ensures that its privacy practices are publicly available through organizational Web sites or otherwise. Supplemental Guidance Organizations employ different mechanisms for informing the public about their privacy practices including, but not limited to, Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), privacy reports, publicly available web pages, email distributions, blogs, and periodic publications (e.g., quarterly newsletters). Organizations also employ publicly facing email addresses and/or phone lines that enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices. Related control: AR-6. References: The Privacy Act of 1974, 5 U.S.C. § 552a; Section 208, E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 10-23.	
	Implementation: (a) All DHS privacy compliance documentation is published on the public-facing website, www.dhs.gov/privacy. (b) All DHS privacy policies and public reports are published on the public-facing website, www.dhs.gov/privacy. Responsible Entitles: (a) DHS Chief Privacy Officer (b) DHS Chief Privacy Officer	
	Implementation Status: Implemented	Note: INSERTPIA and INSERTSORN complete and on file with DHS PRIV.
2.25	Internal Use	PRIV-UL-1
	Control: Internal Use The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices. Supplemental Guidance Organizations take steps to ensure that they use PII only for legally authorized purposes and in a manner compatible with uses identified in the Privacy Act and/or in public notices. These steps include monitoring and auditing organizational use of PII and training organizational personnel on the authorized uses of PII. With guidance from the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and where appropriate, legal counsel, organizations document processes and procedures for evaluating any proposed new uses of PII to assess whether they fall within the scope of the organizational authorities. Where appropriate, organizations obtain consent from individuals for the new use(s) of PII. Related controls: AP-2, AR-2, AR-3, AR-4, AR-5, IP-1, TR-1, TR-2.	

	References: The Privacy Act of 1974, 5 U.S.C. § 552a (b)(1).	
	Implementation: PIA section 3.0 requires System/Program owners to describe how and why the System/Program uses the information. System/Program owners must discuss the intra-Departmental sharing of information. Identify and list the name(s) of any components or directorates within the Department with which the information is shared. Consistent with the Privacy Act, all internal sharing must be consistent with the Privacy Act, 5 U.S.C. § 552a(b)(1) and the "OneDHS" Memorandum (February 1, 2007) which requires that "information shall be shared within DHS whenever the requesting officer or employee has an authorized purpose for accessing the information in the performance of his or her duties, possesses the requisite security clearance, and assures adequate safeguarding and protection of the information. Responsible Entitles: System/Program Owner	
	Implementation Status: Implemented	Note: INSERTPIA and INSERTSORN complete and on file with DHS PRIV.
2.26	Information Sharing with Third Parties	PRIV-UL-2
	Control: Information Sharing with Third Parties The organization: (a) Shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes; (b) Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used; (c) Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and (d) Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required. Supplemental Guidance The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) 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 organizational public notice(s). When a proposed new instance of external sharing of PII is not currently authorized by the Privacy Act and/or specified in a notice, organizations evaluate whether the proposed external sharing is compatible with the purpose(s) specified in the notice. If the proposed sharing is compatible, organizations review, update, and republish their Privacy Impact Assessments (PIAs), System of Records Notices (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. Related controls: AR-3, AR-4, AR-5, AR-8, AP-2, DI-1, DI-2, IP-1, TR-1. References: The Privacy Act of 1974, 5 U.S.C. § 552a (a)(7), (b), (c), (e)(3)(C), (o); ISE Privacy Guidelines.	
	Implementation: (a) PIA section 6.2 requires System/Program owners to describe how external sharing is compatible with their identified SORNs. System/Program owners must also describe which Routine Uses allow for the external sharing. (b) Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001, Component Privacy Officers or PPOCs, the Office for Civil Rights and Civil Liberties, and the Office of the General Counsel should be involved in all phases of ISAA development. Component Privacy Officers, PPOCs, or other DHS employees, as appropriate, submit all proposed interagency ISAAs involving PII to the Chief Privacy Officer for review and approval prior to finalizing an agreement. The Office of Policy submits all proposed international ISAAs to the Chief Privacy Officer for review and approval. The Chief Privacy Officer reviews all proposed ISAAs and works with the relevant Component Privacy Officer or PPOC , or the Office of International Affairs, as appropriate, to ensure that such agreements are amended, where necessary, to fully comply with DHS privacy policy and ISAA guidance. (c)(1) Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001, new DHS Headquarters Component employees (other than Federal Law Enforcement Training Center employees) receive in-class privacy training provided by the Chief Privacy Officer during their orientation and six months thereafter. All DHS employees and contractors complete annual online	

	privacy training developed by the Chief Privacy Officer or by Component Privacy Officers or PPOCs in consultation with the Chief Privacy Officer. (c)(2) Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001, employees who handle Sensitive PII receive additional, role-based privacy training developed by System Managers or Program Managers in consultation with Component Privacy Officers or PPOCs and the Chief Privacy Officer. (d)(1) Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001, Component Privacy Officers or PPOCs, the Office for Civil Rights and Civil Liberties, and the Office of the General Counsel should be involved in all phases of ISAA development. Component Privacy Officers, PPOCs, or other DHS employees, as appropriate, submit all proposed interagency ISAAs involving PII to the Chief Privacy Officer for review and approval prior to finalizing an agreement. The Office of Policy submits all proposed international ISAAs to the Chief Privacy Officer for review and approval. (d)(2) Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001, the Chief Privacy Officer reviews all proposed ISAAs and works with the relevant Component Privacy Officer or PPOC , or the Office of International Affairs, as appropriate, to ensure that such agreements are amended, where necessary, to fully comply with DHS privacy policy and ISAA guidance. Responsible Entitles: (a) System/Program Owner (b) System/Program Owner (c)(1) DHS Chief Privacy Officer (c)(2) System/Program Owner (d)(1) System/Program Owner (d)(2) DHS Chief Privacy Officer	
	Implementation Status: Implemented	Note: INSERTPIA and INSERTSORN complete and on file with DHS PRIV.

3.0 DHS Privacy Office Review

We have reviewed the System Privacy Plan for FIRST RESPONDER COMMUNITIES OF PRACTICE and have made the determination that the privacy controls selected for this system are in fact adequate to satisfy the privacy requirements of NIST SP 800-53 Appendix J, Privacy Controls. For questions, please contact the DHS Privacy Office Compliance Team at 202-343-1717.

[Date]

{*Insert System Owner signature block*}

[Date]

{*Insert Component CISO/ISSM signature block*}

[Date]

{*Insert Authorizing Official signature block}*

Lindsay Vogel 3/7/2018

{*Insert Authorizing Official signature block}*