Privacy Procedural Guide: Personally Identifiable Information (PII) Processing and Transparency (PT) Controls
CIO-IT Privacy-24-01

Initial Release

December 1, 2023

Enterprise Data Governance and Privacy Division

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Initial Release – December 1, 2023		
N/A	Speidel/ Hasan/ Riordan/ Gerhardt/ Hanna/Henry	Initial release to provide guidance on the NIST SP 800-53, Revision 5 PT control family.	New guide.	N/A
N/A	McCormick/ C.B. Wright/ Klemens	• Formatted guide in accordance with current GSA guidance. • Edited guide in collaboration with the Privacy team.		Throughout

Approval

Privacy Procedural Guide: Personally Identifiable Information (PII) Processing and Transparency (PT) Controls, CIO-Privacy 24-01, Initial Release, is hereby approved for distribution.

DocuSigned by:
Richard Speidel
171D5411183F40A...

Richard Speidel
Chief Privacy Officer

Contact: GSA Enterprise Data Governance and Privacy Division at gsa.privacyact@gsa.gov.

TABLE OF CONTENTS

Note: Hyperlinks in running text will be provided for external sources upon first occurrence in the text and if they link to a location within this document (i.e., a different section).

1 Introduction

The General Services Administration (GSA) follows the requirements of the Privacy Act of 1974 which protects Personally Identifiable Information (PII) that GSA maintains in Systems of Records (SOR). A SOR is a file, database, or program from which personal information is retrieved by name or another personal identifier. The GSA Privacy Act System of Records and Notices (SORN) page identifies systems that contain PII. The SORNs are reviewed periodically to ensure they are relevant, necessary, accurate, up-to-date, and covered by the appropriate legal or regulatory authority.

GSA uses Privacy Impact Assessments (PIA) as required by the E-Government Act of 2002 to ensure that privacy issues and protections are addressed within systems that contain PII.

GSA protects PII security and confidentiality through various methods including security technologies and strict access controls. The GSA Privacy Act Program establishes processes and procedures and assigns responsibilities for fulfilling the Privacy Act's mandate. Also published are GSA's privacy policies and practices as they apply to GSA employees, contract requirements, contractors, clients, and other members of the public.

1.1 Purpose

This privacy control guide incorporates by reference the GSA Privacy Act Program website as the official employee reference vehicle for GSA's privacy program, policy, and procedures. The GSA Privacy Act Program addresses information privacy and security issues, establishes GSA's privacy policies and procedures, provides guidance and direction on implementing program requirements, defines privacy-related contracting requirements, and assigns responsibilities to ensure compliance with the Privacy Act of 1974, as amended, the E-Government Act of 2002, and other applicable laws and regulations.

1.2 Scope

The requirements outlined within this guide apply to and must be followed by all GSA Federal employees and contractors who are involved in the management of GSA information systems that store, process, or transmit PII. All GSA information systems must adhere to the requirements and guidance provided with regards to PII procedures, processes, and methods as described in this guide. Per GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy," a GSA information system is an information system:

- used or operated by GSA; or
- used or operated on behalf of GSA by a contractor of GSA or by another organization.

1.3 Policy

In accordance with the Privacy Act of 1974, privacy protection is both a personal and fundamental right of any individual, whose personally identifiable information (e.g., social security number (SSN), date of birth, home address, personal email address) is collected, maintained, and used by GSA to carry out the agency mission and responsibilities and to provide services. OMB Circular A-130, "Managing Information as a Strategic Resource," defines PII as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. GSA's

policy is to safeguard personal information as mandated by laws and regulations. The GSA Privacy Act Program promulgates GSA policy for ensuring compliance with legal requirements to protect PII.

CIO 2100.1 contains the following policy statements regarding protecting PII.

CHAPTER 1: THE GSA INFORMATION TECHNOLOGY SECURITY PROGRAM

9. Privacy Act Systems. In addition to the security requirements in this Order, systems that contain Privacy Act data or PII must implement the privacy controls as defined in NIST SP 800-53 Revision 5 and GSA Order CIO 1878.3 CHGE 1.

13. Cloud Services.

c. The use of PII can only be involved in such products/services when the ATO grants such authorization specifically. PII shall never be introduced into any pilot program at any time.

CHAPTER 4: POLICY FOR PROTECT FUNCTION

1. Identity Management, Authentication and Access Control.

t. Remote access/endpoint security.

(1) Personal computers and/or contractor computers will only be allowed access to the Citrix NetScaler and will not have the ability to map local drives (contingent on passing the scans noted above). No PII or other data deemed sensitive by the data owner shall be stored on non-GFE.

pp. System and/or data owners must verify that data extracts containing PII are handled IAW the GSA Rules of Behavior for Handling PII (CIO P 2180.2). PII must only be disclosed on a need-to-know basis within GSA and disposed of IAW the applicable records retention schedule.

3. Data Security.

a. All PII/CUI and PCI data, and business sensitive data as determined by the AO, and authenticators, including but not limited to passwords, tokens, keys, certificates, and hashes must be encrypted everywhere (i.e., at file level, database level, at rest, and in transit). Encryption algorithms and modules must be FIPS 140-3/140-2 validated.

(1) For databases, encryption of the whole database, table, column, or field levels is acceptable, as appropriate. Other methods including, but not limited to, application encryption or tokenization is also acceptable.
(2) For web services connections, implement end-to-end encryption terminating the connection at the web server; connections terminated at a load balancer shall employ re-encryption techniques to ensure end-to-end encryption.
(3) Internet accessible Websites shall implement HTTPS Only with HTTP Strict Transport Security (HSTS), have no weak ciphers, have no weak protocols, and preload .gov domains.

b. PII/CUI stored on network drives and/or in application databases must have proper access controls (i.e., user identification and authentication) and shall be made available only to those individuals with a valid need-to-know.

f. All sensitive information, such as PII/CUI, as deemed by the data owner, which is transmitted outside the GSA firewall, must be encrypted. Validated encryption modules must be used IAW FIPS 140-3/140-2.

g. An employee or contractor shall not physically take PII from GSA facilities (including GSA managed programs housed at contractor facilities under contract), or access remotely (i.e., from locations other than GSA facilities), without written permission from the employee's supervisor, the data owner, and the IT system AO. Approvals shall be filed with the employee's supervisor. This applies to electronic media (e.g., laptops, USB drives), paper, and any other media (e.g., CDs, DVDs) that may contain PII.

h. PII/CUI data may only be accessed remotely from GFE or through an approved GSA virtual interface (i.e., Citrix and/or VDI) or a GSA authorized system.

i. If PII/CUI needs to be emailed outside the GSA network encryption is required. Instructions can be found on the privacy web page in the section "Documents for Download." An email will be blocked from transmittal if Social Security Numbers are attempted to be sent unencrypted.

NOTE: Information on emailing PII/CUI has been moved to the Emailing and Mailing CUI web page.

j. If PII/CUI needs to be sent by courier, printed, or faxed several steps should be taken. When sending PII/CUI by courier mark, "signature required" when sending documents. This creates a paper trail in the event items are misplaced or lost. Do not let PII documents sit on a printer where unauthorized employees or contractors can have access to the information. When faxing information, use a secure fax line. If one is not available, contact the office prior to faxing, so they know information is coming, and contact them after transmission to ensure they received it. For each event, the best course of action is to limit access to PII/CUI only to those individuals authorized to handle it, create a paper trail, and verify information reached its destination.

NOTE: Information on mailing PII/CUI has been moved to the Emailing and Mailing CUI web page. Information on printing/faxing PII/CUI has been moved to the Printing and Faxing CUI web page.

1.4 References

Federal Laws, Standards, Regulations, and Publications

- 32 CFR Part 2002, "Controlled Unclassified Information"
- Executive Order 13556, "Controlled Unclassified Information"
- FIPS 140-3, "Security Requirements for Cryptographic Modules"
- FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems"
- NIST SP 800-37, Revision 2, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy"

- NIST SP 800-53, Revision 5, “Security and Privacy Controls for Information Systems and Organizations”
- NIST SP 800-63-3, “Digital Identity Guidelines, Revision 3”
- OMB Circular A-108, “Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act”
- OMB Circular A-130, “Managing Information as a Strategic Resource”
- OMB Memorandum M-17-12, “Preparing for and Responding to a Breach of Personally Identifiable Information”
- E-Government Act of 2002
- Privacy Act of 1974

GSA Policies, Procedures, Guidance

- CIO-IT Security-01-02: Incident Response (IR)
- CIO-IT Security-09-44: Plan of Action and Milestones (POA&M)
- CIO-IT Security-09-48: Security and Privacy Requirements for IT Acquisition Efforts
- CIO-IT Security-19-101: External Information System Monitoring
- CIO-IT Security-21-112: Protecting CUI in Nonfederal Systems and Organizations Process
- GSA Emailing and Mailing CUI
- GSA Order CIO 1878.3, “Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices”
- GSA Order CIO 2100.1, “GSA Information Technology (IT) Security Policy”
- GSA Order CIO 2103.2,“Controlled Unclassified Information (CUI) Policy”
- GSA Order CIO 2180.2, “GSA Rules of Behavior for Handling Personally Identifiable Information (PII)”
- GSA Order CIO 2200.1, “GSA Privacy Act Program”
- GSA Order CIO 2231.1, “GSA Data Release Policy”
- GSA Order CIO 9297.2C CHGE 1, “GSA Information Breach Notification Policy”
- GSA Printing and Faxing CUI
- GSA Privacy and Contract Requirements
- GSA Privacy Act Program
- Privacy Act and GSA Employees
- GSA Privacy Impact Assessments (PIA)
- GSA System of Records Notices (SORNs) – Privacy Act

2 Roles and Responsibilities

There are many roles associated with effectively preserving and enhancing privacy protections for information systems that handle PII. The roles and responsibilities provided in this section have been extracted or paraphrased from CIO 2100.1 or summarized from GSA and Federal guidance. The responsibilities listed in this guide are focused on how PII is protected and preserved. Throughout this guide, specific processes and procedures for implementing the PT controls issued by National Institute of Standards and Technology (NIST) are described.

2.1 Senior Agency Official for Privacy (SAOP)

The SAOP has overall responsibility for establishing and overseeing the Privacy Act Program in GSA and for ensuring GSA's compliance with privacy laws, regulations, and GSA policy. Responsibilities include the following:

- Ensures that Privacy Threshold Analyses (PTAs), Privacy Impact Assessments (PIAs), Privacy Act statements, and System of Records Notices (SORNs) are reviewed for privacy issues and meet applicable privacy requirements.
- Reviews and approves system categorizations for systems that are creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and/or disposing of information in identifiable form .
- Oversees privacy control assessments as part of the PIA approval process in accordance with the Authorization to Operate (ATO) cycle.
- Reviews authorization packages for GSA IT systems that are creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and/or disposing of information in identifiable form.
- Signs the transmittal to submit GSA Privacy Act System of Record Notices for publication in the Federal Register to solicit public comments.
- Reports to OMB and Congress on the establishment or significant modification of Privacy Act systems of record.
- Periodically reports to OMB on GSA Privacy Act activities, as required by law and OMB information requests.
- Heads the Full Response Team when responding to major breaches.
- Collaborates with the Evaluation Officer to assess GSA's skills and capacity to resource, produce and use evidence to meet its mission goals, including privacy expertise.
- Assesses the agency's privacy workforce needs and advises the Office of Human Resource Management (OHRM) on hiring personnel, in accordance with GSA's Privacy Continuous Monitoring Strategy and the Federal Privacy Council and Office of Personnel Management's "Toolkit for Recruiting, Hiring, and Retaining Privacy Professionals in the Federal Government."

2.2 Chief Privacy Officer (CPO)

The CPO is responsible for coordinating the implementation of Privacy Act Program requirements within GSA. Responsibilities include the following:

- Develops and issues GSA's Privacy Act policy, standards, and procedures.
- Under the direction of the SAOP, evaluates PIAs, Privacy Act statements, and SORNs for completeness of privacy-related information. Assists in the development of SORNs when applicable.
- Coordinates the concurrence and approval of SORNs for submission to OMB and Congress.
- Submits GSA Privacy Act SORNs for publication in the Federal Register to solicit public comment.
- Submits new and revised systems of record to OMB and Congress for review.
- Develops and clears requests for computer matching systems.
- Reviews forms and other data collection instruments for Privacy Act statements.
- Serves as a liaison with the Office of General Counsel (OGC) on privacy matters.
- Maintains Privacy Act records and documentation.
- Prepares and submits Privacy Act, Computer Matching, and other reports to OMB as required.

2.3 Privacy Analyst (PA)

The PA is responsible for ensuring implementation of adequate privacy for a system in order to document, mitigate, and minimize the privacy risks associated with creating, collecting, using,

processing, storing, maintaining, disseminating, disclosing, and/or disposing of information in identifiable form. A PA must be assigned for every information system. A PA may have responsibility for more than one system, provided there is no conflict. The PA must be knowledgeable of the PII and processes supported by the system. PAs receive notification to complete review of PTAs/PIAs when they are generated by the Archer Governance, Risk, and Compliance (GRC) tool. Responsibilities include the following:

- Reviews and finalizes system PTAs.
- Oversees the review of PT family controls for systems containing PII.
- Advises System Owners of privacy risks to their systems and obtains assistance from the CPO, if necessary, in assessing privacy risk.
- Evaluates PTAs to ensure they meet privacy requirements.
- Prepares and submits Privacy Act systems of record, Computer Matching notices, and other reports to OMB as required.
- Works to develop, revise, and rescind SORNs.
- Investigates and reports on PII incidents. Recommends mitigation action when applicable.
- Reviews outbound, unencrypted emails to non-GSA addresses that appear to contain Social Security Numbers (SSNs) via GSA's Data Loss Prevention (DLP) solution.
- Assists with the development of GSA's Privacy policy, standards, and procedures.

2.4 Chief Information Security Officer (CISO)

The CISO is responsible for implementing IT security management in GSA, with overall responsibility for the GSA IT Security Program, and for security policy on electronic privacy data. Responsibilities include the following:

- Oversees security policy for privacy data.
- Ensures review of PIA for information security considerations.
- Ensures that PIAs are part of GSA's System Development Life Cycle Guidance for Information Technology.

2.5 Authorizing Official (AO)

An AO is the Federal Government management official who is responsible for identifying the level of acceptable risk for an information system, application, or set of common controls and determining whether an acceptable level of risk has been achieved. Final authority to operate or not operate for an information system, application, or a set of common controls rests with the AO. An AO must be assigned to every information system. An AO may have responsibility for more than one system, provided there is no conflict. Responsibilities include the following:

- Ensures IT systems handling privacy data meet the privacy and security requirements of the Privacy Act and IT information security laws and regulations. This includes CIO 2200.1, CIO 1878.3, and NIST SP 800-53, Revision 5.
- Reviews PTAs/PIAs for information systems and applications under their purview.
- Ensures privacy management is included in management planning, programming budgets, and the IT Capital Planning process.
- Ensures IT systems handling privacy data meet the privacy and security requirements of the Privacy Act and IT information security laws and regulations. This includes CIO 2200.1, CIO 1878.3, and NIST SP 800-53, Revision 5.

- Ensures all incidents involving data breaches which could result in identity theft are coordinated through OCISO and the GSA Full Response Team using the GSA breach notification plan per OMB M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," CIO-IT Security-01-02: Incident Response (IR), and GSA Order CIO 9297.2C CHGE 1, "GSA Information Breach Notification Policy."
- Coordinates with the CISO, experts within the OCISO, and the GSA Privacy Office, regarding the consistent management of privacy risks across GSA.

2.6 Information System Security Manager (ISSM)

The ISSM serves as an intermediary to the System Owner and the OCISO Director responsible for ISSO services. There is at least one ISSM per AO. The ISSM reports to the OCISO ISSO Support Division (IST) Director regarding the security and privacy of the systems under their purview. An individual appointed as ISSM for a system cannot also be assigned as the ISSO for the same system. ISSMs must be Federal employees. Responsibilities include the following:

- Manages system assessments (including A&A package requirements and PCI DSS Report on Compliance [for IT systems that process, store, or transmit payment card data or purchase/credit card numbers]), and forwards them to the AO and appropriate OCISO Directors.
- Complies with GSA security and privacy awareness training requirements for individuals with significant security responsibilities.
- Reviews and approves or rejects the PIA.

2.7 Information System Security Officer (ISSO)

The ISSO is responsible for ensuring implementation of adequate system security in order to prevent, detect, and recover from security and/or privacy breaches. An ISSO must be assigned for every FISMA system. An ISSO may have responsibility for more than one system, provided there is no conflict. An individual assigned as the ISSO cannot also be the ISSM or System Owner for the same system. ISSOs may be Federal employees or contractors. The ISSO must be knowledgeable of the information and processes supported by the system. Responsibilities include the following:

- Ensures the system is operated, used, maintained, and disposed of in accordance with documented privacy policies and procedures. Necessary privacy controls should be in place and operating as intended.
- Assists the AO, Data Owner, and Contracting Officer/Contracting Officer Representative (CO/COR) in ensuring users have the required background investigations, the required authorization and need-to-know, and are familiar with internal security and privacy practices before access is granted to the system.
- Complies with GSA security and privacy awareness training requirements for individuals with significant security responsibilities and handling PII.
- Works with the System Owner to complete the PTA for approval.
- Assists in the identification, implementation, and assessment of a system's security and privacy controls, including common controls.

2.8 System Owner

The System Owner is responsible for ensuring that any GSA IT system under their jurisdiction undergoes a PTA, reporting any change that may impact the privacy posture of the system

under their jurisdiction, and, as necessary, completing and updating PIAs. This responsibility includes coordinating with the system manager, system developer, and others who may have a concern about resolving privacy and security issues and reviewing and approving the PTA and/or PIA before submission to a higher level of authority. Responsibilities include the following:

- Ensures systems and the data each system processes have necessary security and privacy controls in place and are operating as intended and protected in accordance with GSA regulations and any additional guidelines established by the OCISO and relayed by the ISSO or ISSM.
- Participates in activities related to the A&A of the system to include security and privacy planning, risk assessments, security and incident response testing, configuration management, and contingency planning and testing.
- Ensures IT security and privacy requirements are included in IT contracts or contracts including IT.
- Conducts PTAs on all systems to ascertain whether the system collects information on individuals or when new systems are developed, acquired, or purchased; performing PIAs when applicable.
- Ensures that GSA has a SORN in place for any SOR under their purview.
- Reviews and modifies SORN(s) under their purview when any significant changes are made, including, but not limited to, significant architectural changes of the system and/or changes to the types and amount of data collected.
- Ensures privacy is planned, documented, and integrated into the system development life cycle from the information system's initiation phase to the system's disposal phase.
- Reviews the privacy controls for their systems and networks annually as part of the FISMA self-assessment, when significant changes are made to the system and network, and at least every three years or via continuous monitoring if the system is in GSA's information security continuous monitoring program.
- Ensures physical or environmental security requirements are implemented for facilities and equipment used for processing, transmitting, or storing sensitive information based on the level of risk.
- Ensures system users and support personnel receive the requisite security and privacy awareness training (e.g., instruction in system rules of behavior).
- Supports the privacy measures and goals established by the CPO.
- Complies with GSA security and privacy awareness training requirements for individuals with significant security responsibilities.
- Integrates and explicitly identifies privacy funding for information systems and programs into IT investment and budgeting plans.
- Coordinates with IT privacy personnel, including the Privacy Analyst, the CPO, and Data Owners, to ensure implementation of system and data privacy requirements.
- Works with the Data Owner, granting access to the information system based on a valid need-to-know/need-to-share that is determined during the account authorization process and the intended system usage.
- Works with Data Owners to audit user activity for indications of fraud, misconduct, or other irregularities when PII may be involved.
- Works with the OCISO and Data Owners to respond to any information PII incidents that impact the system or the data stored within the system.
- Participates as a member of the GSA Full Response Team as defined in GSA Order CIO 9297.2C CHGE 1 to determine if a major incident has occurred.

2.9 Data Owner

The Data Owner owns the information but not the system, application, or platform on which the information is stored, transmitted, or processed. Responsibilities include the following:

- Works with the System Owner, with assistance from the ISSO, to ensure system access is restricted to authorized users who have completed required background investigations, are familiar with internal security and privacy practices, and have completed requisite security awareness training programs (e.g., the annual IT Security and Privacy Awareness course).
- Ensures that data is not processed on a system with security and privacy controls that are not commensurate with the sensitivity of the data.
- Ensures information systems that allow authentication of users for the purpose of conducting Government business electronically complete a Digital Identity Acceptance Statement for digital transactions resulting in an assurance level classification in accordance with NIST SP 800-63-3, “Digital Identity Guidelines, Revision 3” and CIO 2100.1.
- Coordinates with IT security personnel including the ISSM, ISSO, and System Owners to ensure implementation of system and data security requirements.

2.10 Custodian

Custodians own the hardware platforms and equipment on which the data is processed. They are the individuals in physical or logical possession of information from Data Owners. They are responsible for coordinating with Data Owners and System Owners to ensure PII is properly stored, maintained, and protected.

3 GSA Implementation Guidance for Privacy Controls

In the implementation guidance text, the GSA-defined parameter settings included in the control requirements are in blue, italicized text and offset by brackets. As stated in Section 1.2, Scope, the requirements outlined within this guide apply to all GSA systems and must be followed by all GSA Federal employees and contractors involved in the management of GSA information systems that store, process, or transmit PII. The GSA implementation guidance stated for each control applies to personnel and/or the information systems operated on behalf of GSA. Any additional instructions or requirements for contractor systems will be noted in a “Vendor/ Contractor System-Specific Expectation” portion of each control section.

Table 3-1 identifies the designation of PT controls as Common, Hybrid, or System-Specific Controls for both Federal and Contractor systems that store, process, or transmit PII. Effectively, common controls are provided by GSA at the enterprise level or by one of GSA’s Major Information Systems (e.g., General Support System). System specific controls are implemented at the system level, and hybrid controls have shared responsibilities. CIO-IT Security-18-90: Common Control Catalog, describes the GSA enterprise-wide common and hybrid controls and outlines the responsible parties for implementing them.

Table 3-1. Designation of Privacy Controls

Control Type	Federal	Contractor
Common	PT-1	
Hybrid	PT-2, PT-3, PT-4, PT-5, PT-5(2), PT-6, PT-6(1), PT-6(2), PT-7(1), PT-7(2), PT-8	PT-1, PT-2, PT-3, PT-4, PT-5, PT-5(2), PT-6, PT-6(1), PT-6(2), PT-7(1), PT-7(2), PT-8
System-Specific	PT-7	PT-7

Table 3-2 identifies GSA PT control applicability at the FIPS 199 Moderate, and High levels for those systems that store, process, or transmit PII.

Table 3-2. Designation of PT Control Applicability

FIPS 199 Level	Control ID
Moderate	PT-1, PT-2, PT-3, PT-4, PT-5, PT-5(2), PT-6, PT-6(1), PT-6(2), PT-7, PT-7(1), PT-7(2), PT-8
High	PT-1, PT-2, PT-3, PT-4, PT-5, PT-5(2), PT-6, PT-6(1), PT-6(2), PT-7, PT-7(1), PT-7(2), PT-8
MiSaaS	PT-3, PT-4, PT-5, PT-5(2), PT-6

3.1 PT-1 (Privacy and Transparency) Policy and Procedures

Control:

a. Develop, document, and disseminate to [*personnel with privacy responsibilities as defined in GSA CIO Order 2100.1*]:

   1. [*Organization-level*] personally identifiable information processing and transparency policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls;

b. Designate an [*Chief Privacy Officer*] to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy and procedures; and

c. Review and update the current personally identifiable information processing and transparency:

   1. Policy [*annually, as part of the Privacy Program review*], and following [*changes to Federal or GSA policies, requirements, or guidance*]; and

   2. Procedures [*as part of the ATO review/renewal process*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A Process is listed in Table 3-2.

Federal System Common Control Implementation

The GSA Privacy Office develops, disseminates, and implements operational privacy policies that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII. They are disseminated via the Privacy InSite page. The policies and procedures on the Privacy page address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The Privacy policies, procedures, and processes are consistent with Federal laws, orders, directives, regulations, policies, standards, and guidelines.

The GSA Privacy Office develops, disseminates, and implements operational privacy procedures (e.g., PTA, PIA, and SORN processes) via the Privacy InSite page that provide guidance for processing PII and complying with associated privacy controls.

GSA has a designated CPO and SAOP and allocates sufficient resources to implement and operate the organization-wide privacy program. The CPO leads the GSA Privacy Division which develops privacy policies and manages the GSA privacy program.

The GSA Privacy Division is responsible for reviewing and updating GSA Order CIO 2200.1 annually. The GSA Privacy Division is responsible for reviewing and updating CIO-IT Privacy-24-01 (this guide) every three years and following changes to Federal or GSA policies, requirements, or guidance.

Vendor/Contractor System-Specific Expectation: Vendors/Contractors must use GSA policies and guides regarding PII Processing policies and procedures. They may supplement them with their own PII Processing policies and procedures with the approval of the CPO (and the SAOP).

3.2 PT-2 Authority to Process Personally Identifiable Information

Control:

a. Determine and document the [*authority as defined in the SORN and/or PIA*] that permits the [*processing as defined in the SORN and/or PIA*] of personally identifiable information; and

b. Restrict the [*processing as defined in the SORN and/or PIA*] of personally identifiable information to only that which is authorized.

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A Process is listed in Table 3-2.

Privacy Office Common Control Implementation
The GSA Privacy Office provides guidance and oversight to SOs and Data Owners in documenting their Privacy Act SORN. The standard format of the GSA SORN requires the identification of the specific authority that permits the processing of the personally identifiable information.

The individual must provide information in order to verify eligibility to access controlled systems or facilities. All collections are voluntary. Collections may be listed as "mandatory" only if the person is required by law to provide the data and the person is subject to a penalty for refusing. Only the minimum required information is collected in order to provide access.

Federal and Vendor/Contractor System-Specific Expectation
System and Data Owners are responsible for determining and documenting the legal authority permitting the handling of PII data within a SORN, pursuant to 5 U.S.C. §552a (e) (3). When drafting a Privacy Act Statement for review by the GSA Privacy Office, the System Owner must include the legal authority for the collection, creation, storage, use, etc. of the information. System Owners are responsible for ensuring only authorized PII data is processed by the system per its documented SORN.

3.3 PT-3 Personally Identifiable Information Processing Purposes

Control:

a. Identify and document the [*purposes in the PIA and/or SORN*] for processing personally identifiable information;

b. Describe the purpose(s) in the public privacy notices and policies of the organization;

c. Restrict the [*processing*] of personally identifiable information to only that which is compatible with the identified purpose(s); and

d. Monitor changes in processing personally identifiable information and implement [*PTA, PIA and SORN processes*] to ensure that any changes are made in accordance with [*CIO Order 1878.3*].

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A Process is listed in Table 3-2.

Privacy Office Common Control Implementation
The GSA Privacy Office provides guidance and oversight to System Owners in documenting their Privacy Act SORN. The standard format of the GSA SORN requires the identification of the purpose for processing of the personally identifiable information.

The GSA Privacy Office develops privacy policies and manages the GSA Privacy Program. The GSA privacy training and the GSA requirements for PIAs and SORNs ensure that GSA uses PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.

The GSA Privacy Office develops and collaborates with necessary Services and Staff Offices (SSOs) to develop privacy policies and manage the GSA Privacy Program. GSA Orders CIO 2180.2, "Rules of Behavior for Handling Personally Identifiable Information (PII)" and CIO 2100.1 ensure that GSA is in accordance with applicable laws and NIST recommendations with regard to sharing information with third parties. Personal information used to determine employee rights, benefits, and privileges is collected directly from the individual of record whenever possible, and used only for the purpose for which it is intended. The System Owner of each system of records must set up technical, administrative, and physical security measures for processing, storing, transmitting, and disposing of information in the system. All employees

or contractors who work with a system's information as part of their job must follow these measures. Security measures for paper records include storage in secure cabinets or rooms, with access limited to authorized personnel. Electronic records are protected by passwords, firewalls, and other administrative, technical, and physical security measures determined to be necessary by the system manager and program officials, pursuant to 5 U.S.C. §552a (e) (10).

The ISSO is responsible for coordinating the annual review and updating the system/application PIA in GSA's Governance, Risk, and Compliance (GRC) system/tool (currently Archer). PIAs, PTAs, and SORNs must be reviewed and recertified in accordance with the ATO reauthorization cycle of the FISMA system, or when there is a significant system change.

Federal and Vendor/Contractor System-Specific Expectation
When drafting a Privacy Act Statement for review by the GSA Privacy Office, the System Owner must include the purpose(s) for collecting the information. The System Owner is responsible for ensuring that PII is shared only for the authorized purpose(s) identified in the appropriate documentation (SORN, PTA, and/or PIA). The System Owner is responsible for ensuring that updates are made in coordination with the ISSO or that if there are no significant changes to the PII in the system, that the PIA is recertified.

3.4 PT-4 Consent

Control

Implement [*Privacy Act statements*] for individuals to consent to the processing of their personally identifiable information prior to its collection that facilitate individuals' informed decision-making.

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A Process is listed in Table 3-2.

Privacy Office Common Control Implementation
The GSA Privacy Office develops privacy policies and manages the GSA privacy program which provides a means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of PII prior to its collection.

GSA Orders CIO 2200.1, "GSA Privacy Act Program" and CIO 2180.2, "GSA Rules of Behavior for Handling Personally Identifiable Information (PII)," provide 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.

The GSA Privacy Office advises the System Owner on how to obtain consent, where feasible and appropriate, from individuals prior to any new uses or disclosures of previously collected PII.

The GSA Privacy Act Program 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.

Federal and Vendor/Contractor System-Specific Expectation

System Owners are responsible for adding Privacy Act Statements to their systems at the point of collection. Upon request the GSA Privacy Office can provide a template for draft Privacy Act Statements.

3.5 PT-5 Privacy Notice

Control: Provide notice to individuals about the processing of personally identifiable information that:

a. Is available to individuals upon first interacting with an organization, and subsequently at [*whenever PII is collected, updated, or disclosed*];

b. Is clear and easy-to-understand, expressing information about personally identifiable information processing in plain language;

c. Identifies the authority that authorizes the processing of personally identifiable information;

d. Identifies the purposes for which personally identifiable information is to be processed; and

e. Includes [*information in the PII infographic available at the InSite Privacy PII page*].

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A Process is listed in Table 3-2.

Privacy Office Common Control Implementation

The GSA Privacy Program supplies templates and guidance on to how provide effective notice to the public and to individuals regarding:

a. its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII);

b. authority for collecting PII;

c. the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising those choices; and

d. the ability to access and have PII amended or corrected if necessary. The organization provides real-time and/or layered notice when it collects PII.

GSA complies with The Plain Writing Act of 2010 which requires all federal agencies to write "clear government communication that the public can understand and use."

The GSA privacy program provides templates and guidance on how to describe: 1) the PII the organization collects and the purpose(s) for which it collects that information; 2) how the organization uses PII internally; 3) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; 4) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; 5) how individuals may obtain access to PII; 6) how the PII will be protected; and 7) if necessary, how to create the documentation to publicly disclose GSA use of PII.

Personal information used to determine employee rights, benefits, and privileges must be collected directly from the individual of record whenever possible, and used only for the purpose for which it is intended. If the information needs to come from a third party, the individual's written permission is required. Statutory authority must exist for collecting Social Security Numbers (SSNs) for record systems that use the SSN for identification purposes. SSNs will not be collected for systems without this specific authority.

The term "Personally Identifiable Information," as defined in OMB Circular A-130 means "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."

Federal and Vendor/Contractor System-Specific Expectation: System Owners are responsible for coordinating with the Privacy Program to ensure individuals have the ability to access their PII in accordance with GSA policies/procedures. Additionally, the System Owner is responsible for coordinating with the Privacy Program to ensure privacy notices and the rights of individuals are accurate and kept current.

The GSA Privacy Office develops privacy policies and manages the GSA privacy program. The GSA requirements for SORNs and Privacy Act Statements ensure that GSA is in compliance with applicable laws and NIST recommendations with regard to privacy notice and that notices are provided at the point of collection.

3.6 PT-5(2) Privacy Notice | Privacy Act Statements

Control:

Include Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A Process is listed in Table 3-2.

Privacy Office Common Control Implementation

The GSA Privacy Office and System Owners include Privacy Act Statements on GSA forms that collect Personally Identifiable Information (PII) that are part of a system of record.

Federal and Vendor/Contractor System-Specific Expectation: System Owners are responsible for coordinating with the GSA Privacy Program to ensure SORNs and Privacy Act notices on forms that collect PII are kept current.

3.7 PT-6 System of Records Notice

Control:

For systems that process information that will be maintained in a Privacy Act system of records:

a. Draft system of records notices in accordance with OMB guidance and submit new and significantly modified system of records notices to the OMB and appropriate congressional committees for advance review;

b. Publish system of records notices in the Federal Register; and

c. Keep system of records notices accurate, up-to-date, and scoped in accordance with policy.

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A Process is listed in Table 3-2.

Privacy Office Common Control Implementation
The GSA Privacy Office is responsible for overseeing the process to publish SORNs, with the input and approval of system stakeholders. Using NIST and OMB guidance, the Privacy Office evaluates the need for a new SORN for a given system against revising a currently existing SORN. A "new" system of records is one for which no public notice is currently published in the Federal Register. A new SORN must be published when any one of the following criteria is met:

- A program, authorized by a new or existing statute or Executive Order (EO), maintains information on an individual and retrieves that information by personal identifier.
- There is a new organization of records resulting in the consolidation of two or more existing systems into one new umbrella system, whenever the consolidation cannot be classified under a current SORN.
- It is discovered that records about individuals are being created and used, and that this activity is not covered by a currently published SORN. In this case, OMB requires the temporary suspension of data collection and disclosure.
- A new organization (configuration) of existing records about individuals that was not previously subject to the Privacy Act (i.e., was not a system of records) results in the creation of a system of records.

The GSA Privacy Office publishes SORNs in the Federal Register, subject to required oversight processes, for systems that require coverage by a SORN. When a GSA organization proposes to establish a new system of records or significantly revise an existing one, the program manager should notify the GSA Privacy Office which will provide assistance in preparing a SORN using the prescribed format, coordinate its review and approval within GSA, and submit it for evaluation by OMB and Congress and for publication in the Federal Register.

The GSA Privacy Office and System Owners review the SORNs and recertify in accordance with the ATO reauthorization cycle of the FISMA system(s), and when there is a significant system change, and include Privacy Act Statements on the necessary GSA forms that collect PII. More information regarding SORNs and Privacy Act Statements can be found in 41 CFR Part 105-64.

Federal and Vendor/Contractor System-Specific Expectation: System Owners are responsible for coordinating with the Enterprise Data Governance and Privacy Division to ensure SORNs and Privacy Act notices on forms that collect PII are kept current.

If a significant alteration needs to be made to a system of records, the GSA Privacy Office, in coordination with the System Owner, will amend the existing SORN for that system of records and republish it in the Federal Register to comply with the OMB requirements in Circular A-108 "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act."

3.8 PT-6(1) System of Records Notice | Routine Uses

Control:

Review all routine uses published in the system of records notice at [*any major change*] to ensure continued accuracy, and to ensure that routine uses continue to be compatible with the purpose for which the information was collected.

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A Process is listed in Table 3-2.

Privacy Office Common Control Implementation
Routine uses apply to information sharing external to GSA. The term "routine use" is defined, with respect to the disclosure of a record, as "the use of such a record for a purpose which is compatible with the purpose for which the record was collected." This section describes each situation in which GSA may share records on individuals covered by the SORN under the Privacy Act Section 552a(b)(3). The routine uses must be compatible and consistent with the purpose for which the record was collected. This ensures the public receives adequate notice of the agency's planned uses of the information in the system of records. The following language must be included prior to the list of routine uses: "In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed to authorized entities, as is determined to be relevant and necessary, outside GSA as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:"

Common routine uses for most systems of records include sharing:

- For audits and oversight.
- For congressional inquiries.
- With contractors, grantees, and experts to perform OPM-authorized activities.
- For investigations of potential violations of law.
- For intelligence purposes.
- With the National Archives and Records Administration (NARA) for records management purposes.
- For litigation purposes.
- For data breach and mitigation response.

SORNs must be reviewed and recertified in accordance with the ATO reauthorization cycle of the FISMA system and when there is a significant change to the system.

Federal and Vendor/Contractor System-Specific Expectation: System Owners are responsible for coordinating with the GSA Privacy Program to ensure SORNs and Privacy Act notices on forms that collect PII are kept current.

The Privacy Act requires that a notice describing each System of Records proposed for establishment be published in the Federal Register for review and comment by the public and other interested parties. The notice allows questions to be raised and resolved before the system is put into effect and ensures that privacy considerations have been addressed. GSA complies with the Privacy Act requirements.

3.9 PT-6(2) System of Records Notice | Exemption Rules

Control:

Review all Privacy Act exemptions claimed for the system of records at [*any significant change*] to ensure they remain appropriate and necessary in accordance with law, that they have been promulgated as regulations, and that they are accurately described in the system of records notice.

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A Process is listed in Table 3-2.

Privacy Office Common Control Implementation
There are no exceptions to the SORN process. However, certain exemptions to the Privacy Act can be claimed. The head of GSA may promulgate rules, in accordance with the requirements (including general notice) of sections U.S.C. 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f) of this section.

Federal and Vendor/Contractor System-Specific Expectation: System Owners are responsible for coordinating with the GSA Privacy Program and the Office of General Counsel to ensure that the agency promulgates any Privacy Act exemption as a rule per GSA agency rulemaking procedures. At the time rules are adopted under this subsection, GSA and/or its contractors shall include in the statement required under section 553(c) of The Privacy Act, the reasons why the system of records is to be exempted from a provision of this section of the Privacy Act. Any exemptions taken in a Notice of Proposed Rulemaking must be published as a Final Rule before they are effective. Refer to OMB SORN Guidance in Circular A-108 for further information and specific criteria regarding submission of exemptions.

3.10 PT-7 Specific Categories of Personally Identifiable Information

Control:

Apply [*FIPS validated encryption*] for specific categories of personally identifiable information.

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level is listed in Table 3-2.

Privacy Office Common Control Implementation
System Owners are responsible for ensuring the system deploys FIPS-validated encryption.

Federal and Vendor/Contractor System-Specific Expectation: Vendors/contractors are responsible for ensuring the system deploys FIPS-validated encryption.

3.11 PT-7(1) Specific Categories of Personally Identifiable Information | Social Security Numbers

Control:

When a system processes Social Security numbers:

(a) Eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to their use as a personal identifier;

(b) Do not deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his or her Social Security number; and

(c) Inform any individual who is asked to disclose his or her Social Security number whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A Process is listed in Table 3-2.

Privacy Office Common Control Implementation
System Owners and Data Owners are responsible for eliminating unnecessary collection, maintenance, and use of SSNs, and exploring alternatives to their use as a personal identifier. When drafting a PIA or SORN for review by the GSA Privacy Office, the System Owner must include the legal authority for collecting SSNs and why an alternative cannot be used.

Under the Privacy Act, 1677(a), agencies are prohibited from denying an individual any right, benefit, or privilege provided by law because of the individual's refusal to disclose his or her SSN unless disclosure is required by federal statute.

Section 7 of the Privacy Act (found at 5 U.S.C. § 552a note (Disclosure of Social Security Number)) states, “It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual’s refusal to disclose his social security account number.” Sec. 7(a)(1). GSA is compliant with these regulations.

GSA Privacy Program supplies templates and guidance on to how provide effective notice to the public and to individuals regarding: 1) its activities that impact privacy, including its collection of social security numbers; 2) whether that disclosure is mandatory or voluntary; 3) authority for collecting SSN; 4) how it will be used.

Federal and Vendor/Contractor System-Specific Expectation: System Owners and Data Owners are responsible for eliminating unnecessary collection, maintenance, and use of SSNs, and explore alternatives to their use as a personal identifier. When drafting a PIA or SORN for review by the GSA Privacy Office, the System Owner must include the legal authority for collecting SSNs and why an alternative cannot be used.

3.12 PT-7(2) Specific Categories of Personally Identifiable Information | First Amendment Information

Control:

Prohibit the processing of information describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual or unless pertinent to and within the scope of an authorized law enforcement activity.

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A Process is listed in Table 3-2.

Privacy Office Common Control Implementation
The GSA Privacy Office ensures that GSA uses PII internally only for the authorized purpose(s) identified and reviews processing activities to prohibit the processing of information describing how any individual exercises rights guaranteed by the First Amendment unless expressly

authorized by statute or by the individual or unless pertinent to and within the scope of an authorized law enforcement activity.

Federal and Vendor/Contractor System-Specific Expectation: System Owners are responsible for coordinating with the GSA Privacy Program to ensure that processing activities do not describe how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual or unless pertinent to and within the scope of an authorized law enforcement activity.

3.13 PT-8 Computer Matching Requirements

Control:

When a system or organization processes information for the purpose of conducting a matching program:

a. Obtain approval from the Data Integrity Board to conduct the matching program;

b. Develop and enter into a computer matching agreement;

c. Publish a matching notice in the Federal Register;

d. Independently verify the information produced by the matching program before taking adverse action against an individual, if required; and

e. Provide individuals with notice and an opportunity to contest the findings before taking adverse action against an individual.

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A Process is listed in Table 3-2.

Privacy Office Common Control Implementation
System Owners must notify the GSA Privacy Office in the event that GSA needs to establish computer matching programs or agreements to share system of records information with other Federal or non-Federal agencies. The Data Evidence Governance Board (DEGB) Leads governance body will review and approve such programs and agreements.

System Owners and the GSA Privacy Office are responsible for establishing documentation describing the sharing of personal information among computerized systems of two or more Federal or non-Federal agencies. Generally, the shared information is used to determine the eligibility of individuals for Federal benefit programs or to identify delinquencies on obligations. The Privacy Office is responsible for coordinating the development and clearing requests for computer matching systems and preparing and submitting Privacy Act, Computer Matching, and other reports to OMB as required.

The System Owner is responsible for coordinating with the GSA Privacy Office in preparing a Privacy Act notice for publication in the Federal Register.

The GSA DEGB Leads governance body, headed by the CPO and SAOP, oversees organizational Computer Matching Agreements (CMA) and ensures that any such agreements GSA may enter into are published on a public GSA website.

Appeals of a DEGB Leads governance body denial for a computer matching agreement must be submitted to the Director of OMB. GSA complies with the requirements of the Privacy Act to afford individuals the right to privacy of records that are maintained in systems of records and incorporates the provisions of the Computer Matching and Privacy Protection Act of 1988 (Public Law 100-503), including the Computer Matching and Privacy Protection Amendments.

System-Specific Guidance: System Owners must notify the GSA Privacy Office in the event that GSA needs to establish a computer matching program or agreement to share systems of records information with other Federal or non-Federal agencies. The DEGB Leads governance body review and approve such programs and agreements.

The Computer Matching and Privacy Protection Act of 1988 (the Act), Pub.L.100-503, amends the Privacy Act of 1974, and establishes procedural safeguards affecting agencies' use of Privacy Act records in performing certain types of computerized matching programs. The Act regulates the use of computer matching by federal agencies involving personally identifiable records maintained in a system of records subject to the Privacy Act. The Act requires agencies to have written agreements in place specifying the terms under which matches are to be conducted. The Act applies to the computerized comparison of two or more automated systems of records (or federal personnel or payroll systems of records) between federal agencies or between a federal agency and a non-federal agency.

4 Additional Guidance

Where there is a conflict between NIST guidance and GSA guidance, contact the Enterprise Data Governance and Privacy Division for guidance, at gsa.privacyact@gsa.gov.