GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO 1878.3A
December 11, 2023

GSA ORDER

SUBJECT: Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Statements, and System of Records Notices

1. Purpose.

a. This Order issues policies and procedures for identifying and addressing any privacy issues in General Services Administration (GSA) Information Technology (IT) systems. For purposes of this Order, a GSA IT system is an IT system owned or operated by GSA or by a contractor on behalf of GSA, and any IT application, or project containing Personally Identifiable Information (PII).

b. This Order describes the compliance-driven tools to identify and mitigate privacy risks. They include Privacy Threshold Assessments (PTAs), Privacy Impact Assessments (PIAs), Privacy Act Statements, and System of Records Notices (SORNs). This Order also assigns responsibilities to ensure compliance with applicable laws and regulations governing privacy and GSA policies and procedures for conducting and maintaining PTAs, PIAs, Privacy Act Statements, and SORNs as part of an information system's authorization to operate (ATO) package.

2. Background.

a. The Privacy Act of 1974, 5 U.S.C. § 552a "establishes a code of fair information practices" that governs the collection, maintenance, use, and dissemination of personal information by federal executive branch agencies. GSA is required to protect PII in accordance with the Privacy Act. GSA shall identify and address potential privacy risks in all life cycle stages (e.g., initiating, developing/acquiring, operating/maintaining, disposing) of GSA IT systems. In addition, GSA shall identify and mitigate potential privacy risks when contractors handle PII on behalf of GSA.

b. GSA performs a PTA as the means for analyzing whether a GSA IT system collects, maintains, or uses PII for identifying appropriate privacy protection measures. The PTA template is also used to identify other potential categories of Controlled Unclassified Information (CUI).

c. GSA performs a PIA as a key tool to ensure that GSA IT systems appropriately protect the privacy of individuals in accordance with the E-Government Act of 2002, PL 107-347 § 208. GSA's PIA process determines the risks and effects of collecting, maintaining, using, and/or disseminating PII, and it examines and evaluates protections and alternate processes for handling PII to mitigate potential privacy concerns at every life cycle stage (e.g., initiation, development/acquisition, implementation/assessment, operations and maintenance, disposal) in any GSA IT system (including those maintained by contractors). GSA PIAs must comply with OMB M-03-22.

d. GSA uses Privacy Notices and Privacy Act Statements to ensure transparency about the information it is collecting. These notices ensure that GSA informs individuals about the proposed use of the information when asking to collect information and limits its collection of information to that which is legally authorized and necessary.

e. GSA publishes SORNs as required by the Privacy Act of 1974, 5 U.S.C. § 552a. GSA SORNs must comply with OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication Under the Privacy Act*, dated December 23, 2016.

f. GSA includes a system or application's SORN, PIA and/or PTA as part of the authorization to operate (ATO) package, and the timing and conditions of review for those privacy documents are the same as the overall ATO package.

3. Applicability.

a. This Order applies to all GSA employees and contractors. In accordance with GSA IT Security Procedural Guide 09-48, *Security and Privacy Requirements for IT Acquisition Efforts*, and General Services Acquisition Regulation (GSAR) part 511.171, **Requirements for GSA Information Systems**, Contracting Officers (COs) must include compliance with this policy in any contract or task order award.

b. This Order applies to the Office of Inspector General (OIG) to the extent that the OIG determines that this Order is consistent with the OIG's independent authority under the Inspector General (IG) Act (see applicable legal and regulatory requirements), and it does not conflict with other OIG policies or mission.

c. This Order applies to the Civilian Board of Contract Appeals (CBCA) only to the extent that the CBCA determines that this Order is consistent with the CBCA's independent authority under the Contract Disputes Act (see applicable legal and regulatory requirements), and it does not conflict with other CBCA policies or mission.

4. Cancellation. This Order supersedes and cancels 1878.3 CIO CHGE 3 Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices.

5. Explanation of Changes.

a. Updated CPO responsibilities that have been delegated to Privacy Analysts; and

b. Added supporting documentation, updated title, and other administrative changes.

6. Approvals and Reviews.

a. Each Privacy Threshold Assessment (PTA), Privacy Impact Assessment (PIA) and System of Records Notice (SORN) is maintained as part of the authorization to operate (ATO) package;

b. The Project Manager/System Owner, the Information Systems Security Officer (ISSO), and the Privacy Analyst are required to approve PTAs;

c. The Project Manager/System Owner, Information Systems Security Manager (ISSM), and the Chief Privacy Officer (CPO) are required to approve PIAs; and

d. The Program Manager/System Owner is required to review the SORN and must modify it whenever significant changes are planned or take place. The SAOP approves all SORNs prior to publication in the Federal Register.

7. Responsibilities.

a. Authorizing Official (AO). Each Service and Staff Office AO is responsible for ensuring the security of their organization's systems. Additionally, the AOs are responsible for reviewing PIAs for their organization as part of the Authorization to Operate (ATO).

b. Chief Information Officer (CIO). The CIO is responsible for the overall IT security management in GSA.

c. Chief Information Security Officer (CISO). The CISO is responsible for reviewing and approving PIAs as part of the ATO.

d. Chief Privacy Officer (CPO). Under the direction of the SAOP, the CPO is responsible for evaluating the PTAs, PIAs, Privacy Act Statements, and SORNs for completeness of privacy-related information. The CPO approves the PIAs, and along with the SAOP, reviews and approves SORNs before they are published in the Federal Register. PIAs and SORNs are published to gsa.gov/pia and gsa.gov/sorn. The CPO delegates the responsibility of evaluating and signing the PTAs, as well as evaluating Privacy Act Statements, to Privacy Analysts.

e. Privacy Analysts. GSA Privacy Analysts are responsible for evaluating and signing the PTAs, as well as evaluating Privacy Act Statements. While Privacy Analysts do not sign the PIAs and SORNs, they perform a thorough privacy review before PIAs and SORNs are routed for signature. Privacy Analysts also perform the administrative tasks around completing PIAs and SORNs, including but not limited to tracking the status of documentation, requesting publication of finished documents, and preparing transmittal documents.

f. Contracting Officers (CO). GSA COs shall:

(1) Ensure the appropriate privacy and security requirements of this policy are included in any contract or task order award to a GSA contractor performing any work for or providing services for GSA IT systems; and

(2) Ensure the contract allows the Government or its designated representative (e.g., contractor) to review, monitor, test, and evaluate the proper implementation, operation, and maintenance of any privacy controls. This requirement includes but is not limited to documentation review, access controls review, and operational process reviews.

g. Developer/Designer. The system developer/designer is responsible for ensuring that the system design and specifications conform to privacy standards and requirements and that technical controls are in place for safeguarding PII.

h. Heads of Services and Staff Offices (HSSOs). These individuals are responsible for coordinating the efforts of management and technical personnel under their jurisdiction in meeting privacy requirements and goals as well as ensuring their GSA IT systems are compliant with GSA's CUI Policy and guide.

i. Information System Security Manager (ISSM). ISSMs are required to sign any PIAs.

j. Information System Security Officer (ISSO). The ISSO works with the System/Project Manager to complete the PTA and must approve the PTA. ISSOs may also develop PIAs.

k. Program Manager/System Owner.

(1) The Program Manager/System Owner is responsible for ensuring that any GSA IT system under the Program Manager/System Owner's 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.

(2) For GSA SORNs, the Program Manager/System Owner (a.k.a., System Manager as defined in OMB Circular A-108) of the respective GSA IT system is the official who is responsible for ensuring that GSA has a SORN in place for the system of records. Each GSA SORN describes what, why, and how GSA collects, maintains, and uses records in each system of records. The Program Manager/System Owner must review their SORN(s) and modify SORN(s) when any significant changes are made. Examples of significant changes that require a SORN revision include two systems of records being combined into one or a Government-wide SORN covering the records. See OMB Circular A-108, paragraph 6(b), for additional examples of significant changes requiring a SORN modification and paragraph 7(b) for OMB's Standard Review Process for Systems of Records.

l. Senior Agency Official for Privacy (SAOP). The SAOP is responsible for ensuring that PTAs, PIAs, Privacy Act Statements, and SORNs are reviewed for privacy issues and meet applicable privacy requirements. The SAOP or designee shall also review and approve system categorizations for systems with PII, oversee privacy control assessments as part of the ATO process, and review authorization packages for any GSA IT system that collects, maintains, or uses PII. The SAOP or designee also 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.

8. Procedures.

a. Completing the PTA. All GSA IT systems in existence, planned or under development, shall be evaluated through a PTA to document if any types of PII will be/is collected, maintained, and/or used. A new PTA shall be performed for GSA IT systems that do not have a PTA on file with GSA's Privacy Office. Any significant change to any GSA IT system that collects, uses, or maintains PII or plans to collect, use, or maintain PII shall be reported to the GSA Privacy Office. If the GSA IT system already has a PIA in place, such changes must be recorded there. Completed PTAs are reviewed by the Privacy Office to determine whether additional actions are required for transparency and/or risk mitigation purposes.

b. Completing the PIA.

(1) All GSA IT systems, applications, or projects that contain PII are subject to the PIA requirement.

(2) The OMB provides instructions on conducting PIAs in M-03-22; GSA's completed PIAs are available at www.gsa.gov/pia.

c. PTA and PIA timing.

(1) A PTA should be initiated at the earliest possible stage of development of a new GSA IT system when requirements are being analyzed and decisions are being

made about design and data usage.

(2) A PTA for an existing GSA IT system that contains no PII must be reviewed and recertified by the System Owner in coordination with the ISSO aligned to the ATO reauthorization cycle and/or when there is a significant change to the system.

(3) If a GSA IT system requires a PIA, any significant changes to a GSA IT system collecting, maintaining, or using PII must be described to the Privacy Office in proposed updates to the existing PIA by the Program Manager/System Owner.

d. SORNs.

(1) If the Privacy Office determines that a SORN is required, the Program Manager/System Owner shall develop one in accordance with GSA and Office of Management and Budget (OMB) standards.

(2) The Program Manager/System Owner must provide notice to the Privacy Office and update the SORN whenever making a significant change to the system of records (see Section 7(k) above).

(3) After the Program Manager/System Owner drafts a new SORN, revises an existing SORN, or notice of rescindment, the Privacy Office shall review and provide concurrence. Once approved by the Privacy Office, the SORN must receive concurrence from the Office of General Counsel, Office of Strategic Communication (OSC), and Office of Congressional & Intergovernmental Affairs.

Once approved internally, the Privacy Office will report to the Office of Management and Budget (OMB) and Congress any proposal to establish, rescind or significantly modify a system of records at least 30 days prior to the submission of the notice to the *Federal Register* for publication. If GSA receives public comments, the Privacy Office shall review the comments. If GSA thereafter determines that significant changes are necessary, GSA shall make the needed revisions and re-submit for review to the *Federal Register*.

(4) Concurrent with the ATO review process, the Program Manager/System Owner must confirm the SORN is up-to-date and that no significant changes have occurred since initial publication or the last update.

9. Applicable legal and regulatory requirements.

a. CIO 2100.1 GSA Information Technology (IT) Security Policy. This Order identifies the rules and procedures for all individuals accessing and using GSA's IT assets and resources. The Order's objectives are to enable GSA to meet its mission and business objectives by implementing systems with due consideration of IT-related risks to GSA, its partners, and customers. Adherence to the Order is mandatory and will provide assurance of confidentiality, integrity, availability, and accountability by

employing management, operational, and technical security controls as part of risk-mitigation-based management.

b. Executive Order (EO) 13556, Controlled Unclassified Information (CUI). This EO establishes an open and uniform program for managing information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information that is classified under Executive Order 13526,Original Classification Authority.

c. General Services Acquisition Regulation (GSAR) part 511.171. This section of GSA's acquisition regulations requires COs to include compliance with this policy in the contract or task order for contractor employees.

d. Inspector General Act of 1978. This Act created IG positions and offices and gave IGs the authority to review the internal documents of their departments or offices. IGs have the responsibility to investigate fraud, give policy advice, handle certain complaints by employees, and to report to the heads of their agencies and to Congress on their activities every six months.

e. OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act. This circular requires agencies to publish a SORN in the *Federal Register* when establishing a new system of records and when making significant changes or rescinding an existing system of records.

f. OMB Circular A-130, Managing Information as a Strategic Resource. This circular requires Federal agencies to:

(1) Develop, implement, document, maintain, and oversee agency-wide privacy programs that include people, processes, and technologies. Where PII is involved, agencies' privacy programs shall play a key role in information security, records management, strategic planning, budget and acquisition, contractors and third parties, workforce, training, incident response, and implementing the Risk Management Framework; and

(2) Maintain an inventory of PII in the agency's custody, regularly review all PII maintained by the agency, and comply with applicable requirements regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure and disposal of PII. In addition, agencies' privacy programs shall impose, where appropriate, conditions on other agencies and entities to which PII is being disclosed that govern the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of the PII.

g. OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002. This memorandum provides clarification and additional guidance for the privacy provisions of the Act and requires agencies to conduct a PIA before developing or procuring IT systems or projects that collect,

maintain or disseminate PII.

h. OSC 2106.2A GSA Social Media Policy. This Order establishes policy for employee use of social media. It applies to all GSA employees and contractors engaged in social media on behalf of GSA as part of their duties.

i. The Federal Information Security Modernization Act of 2014 (FISMA). FISMA establishes security practices for Federal computer systems and, among its other system security provisions, requires that agencies:

(1) Conduct a periodic assessment of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency; and

(2) Address information privacy throughout the life cycle of agency systems.

j. The E-Government Act of 2002, Section 208. This act aims to ensure privacy in the conduct of Federal information activities and requires agencies to conduct PIAs of electronic information systems.

k. The Privacy Act of 1974 (5 USC 552a). The Privacy Act, as amended, affords individuals the right to privacy of information maintained in systems of records by Federal agencies. The Act incorporates the Computer Matching and Privacy Protection Act of 1988, Public Law 100-503 and the Computer Matching and Privacy Protection Amendments of 1990, which address electronic sharing of information. The Privacy Act specifically states that each agency shall:

(1) Maintain in its records only the information about an individual that is relevant and necessary to accomplish a purpose of the agency as required by statute or Executive Order of the President;

(2) Collect information to the greatest extent practicable directly from the individual when the information may result in adverse determinations about the individual's rights, benefits and privileges under Federal programs;

(3) Maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination; and

(4) Establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity that could result in substantial harm, embarrassment, inconvenience or unfairness to any individual about whom information is maintained.

10. Definitions.

a. GSA Information Technology (IT) system. The electronic information system which is comprised of the hardware and software used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. A GSA IT system refers to any system that is owned or operated by GSA or by a contractor on behalf of GSA, as well as applications and projects containing PII.

b. Individual. A citizen of the United States or a person lawfully admitted for permanent residence.

c. Personally Identifiable Information (PII).

(1) PII is 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. See OMB Circular No. A-130, Managing Federal Information as a Strategic Resource.

(2) The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified using information that is linked or linkable to said individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other information to identify a specific individual, could be used to identify an individual (e.g., Social Security Number (SSN), name, birthday, home address, personal email). More information about handling PII at GSA can be found at this link on InSite (available only to those on GSA's network).

d. Privacy Impact Assessment (PIA). An assessment of how PII is handled:

(1) To ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;

(2) To determine the risks and effects of collecting, maintaining and using PII in an electronic information system; and

(3) To examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

e. Privacy Threshold Assessment (PTA). An assessment of what types of information are collected, maintained, or used by a system, and for what purpose(s).

f. Record. Any item, collection, or grouping of information about an individual that is

maintained by an agency, including but not limited to education, financial transactions, medical history, and criminal or employment history, and that contains the individual's name or identifying number, symbol, or other identifying particular assigned to the individual such as a fingerprint or voiceprint, or a photograph.

g. Significant change. (See OMB Circular No. A-108). As a general matter, significant changes are those that are substantive in nature and therefore warrant a revision of the PTA, PIA and/or SORN in order to provide notice to the public of the character of the modified system of records. Examples of significant changes include:

- A substantial increase in the number, type, or category of individuals about whom records are maintained in the system
- A change that expands the types or categories of records maintained in the system
- A change that modifies the scope of the system
- A change that modifies the purpose(s) for which the information in the system of records is maintained.

h. System of records. A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

11. Signature.

/S/
ZACHARY WHITMAN
Chief Data Officer
Senior Agency Official for Privacy
Office of GSA IT