PRIVACY THRESHOLD ANALYSIS (PTA)

AND

PRIVACY IMPACT ASSESSMENT (PIA)

POLICY

U.S. MERIT SYSTEMS PROTECTION BOARD

September 30, 2019

INTRODUCTION

The U.S. Merit Systems Protection Board (MSPB) is committed to a robust privacy program that ensures the appropriate protection of privacy in the administration of its mission. To facilitate this commitment, MSPB is implementing this Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA) policy. PTAs and PIAs are used by MSPB to identify, evaluate, and mitigate privacy risks throughout the development lifecycle of a program or information system.

MSPB's agency-wide privacy program is located in the Office of the Clerk of the Board and consists of the Senior Agency Official for Privacy (SAOP), Chief Privacy Officer/Director of Information Services, and Privacy Analyst. Together, they form the core "privacy team" that is responsible for coordinating with MSPB program offices to ensure all MSPB systems, programs, and initiatives comply with Federal laws, rules, and policies concerning the appropriate protection of privacy.

WHAT IS A PTA AND WHEN IS IT REQUIRED?

A PTA is a questionnaire used to determine if a system contains personally identifiable information (PII), whether a PIA is required, whether a System of Records Notice (SORN) is required, and if any other privacy requirements apply to the information system. While not required by statute, regulation or guidance, a PTA is a tool that helps MSPB to determine whether an MSPB program or system has privacy implications and whether additional privacy compliance documents are required. The purpose of the PTA is to:

- Identify programs and systems that are privacy-sensitive;
- Demonstrate MSPB's considerations and inclusions of privacy during the review of a program or system;
- Provide a record of the program or system and its privacy requirements to MSPB's privacy team; and
- Demonstrate MSPB's compliance with privacy laws, regulations, and Government-wide guidance.

MSPB begins the privacy compliance process with a PTA, which serves as the official determination by MSPB as to whether an MSPB program or system has privacy implications.[1]

Program managers and system owners should collaborate with the privacy team to complete a PTA whenever they believe a program, system (whether new or substantially changed), or information collection involves PII or privacy-sensitive technologies. A PTA is used by MSPB to determine whether a PIA is required.

[1] Copies of MSPB's PTA and PIA templates may be obtained on MSPB's Portal page for privacy or by or emailing privacy@mspb.gov.

WHAT IS A PIA?

A PIA is required by Section 208 of the E-Government Act of 2002 to ensure sufficient protections for the privacy of personal information. PIAs analyze how MSPB collects, uses, disseminates, and maintains PII, and documents how MSPB incorporates privacy concerns through the development, design, and deployment of a technology, program, or rulemaking. PIAs are used to conduct reviews of how information about individuals is handled within MSPB when we use information technology (IT) to collect PII, when MSPB develops or purchases new IT systems that handle PII, or when there is a substantial change to an IT system that handles PII.[2]

The Office of Management and Budget (OMB) has established a Government-wide policy for managing information as a strategic resource,[3] including a requirement for Federal agencies to ensure compliance with privacy requirements and manage privacy risk. Under this policy, OMB has defined a PIA as

> an analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form[4] in an electronic information system; and to examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns. A privacy impact assessment is both an analysis and a formal document detailing the process and the outcome of the analysis.[5]

MSPB's PIAs demonstrate that we have considered privacy for the lifecycle of a program or system, including the collection, maintenance, dissemination, use, and destruction of information in identifiable form. The PIA process ensures that we have identified and mitigated any privacy risks and that privacy is "baked-in" to the project or system from the start and that we have made system considerations that incorporate privacy into the system architecture.

---

[2] Office of Management and Budget (OMB) Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (OMB M-03-22).
[3] OMB Circular A-130, Managing Information as a Strategic Resource (OMB A-130).
[4] "Information in identifiable form" is defined as information in an IT system or online collection that directly identifies an individual or MSPB intends to use to identify an individual in conjunction with other data elements.
[5] OMB A-130 at Section I.10. 63.

WHEN ARE PIAs REQUIRED?

A PIA should be conducted before

> developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public, or initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government).[6]

After completing a PTA, the privacy team will provide the program manager or system owner with a determination on whether a PIA is required.[7] If it is determined that a PIA is required, a PIA should be drafted by the project manager or system owner in collaboration with the privacy team. PIAs are usually required when:

- Developing or procuring any new technologies or systems that handle or collect PII.
- Creating a new program, system, technology, or information collection that may have privacy implications.
- Updating a system that results in new privacy risks.
- Issuing a new or updated rulemaking that entails the collection of PII.

APPROVAL AND PUBLICATION OF THE PIA

MSPB's privacy team will assist the program office or system owner in preparing the PIA for review by the SAOP, MSPB's designated "reviewing official."[8] Once the PIA has been approved by the SAOP, the PIA should be published on MSPB's external privacy website, located at www.mspb.gov/privacy, unless the PIA would raise security concerns or reveal classified, sensitive, or otherwise protected information.[9]

PAPERWORK REDUCTION ACT (PRA)

If the program manager is seeking to conduct a new electronic collection of information that will handle PII, please contact the privacy team to begin the process set forth in this policy.[10]

---

[6] OMB M-03-22 at Section II.B.a.1-2. PIAs for *Major Information Systems* require more extensive analyses. *See*, *id.* at Section II.C.b.2; OMB A-130 at Section I.5.f and Appendix II-10.

[7] "No PIA is required where information relates to internal government operations, has been previously assessed under an evaluation similar to a PIA, or where privacy issues are unchanged . . . ." For examples of when a PIA is not required, *see* OMB M-03-22 at Section II.B.c.

[8] OMB M-03-22 at Section II.C.c; E-Gov Act at paragraph (b)(B)(ii).

[9] OMB M-03-22 at Section II.C.c; E-Gov Act at paragraph (b)(B)(iii) and (b)(C); OMB A-130 at Appendix II-10.

[10] *See* OMB M-03-22 at Section II.D.

SYSTEM OF RECORDS NOTICE (SORN)

The privacy team shall consider whether a PIA is required when developing or updating a SORN.[11]

UPDATING THE PTAs AND PIAs

A PTA should be reviewed and re-certified every three (3) years. Additionally, a PIA should be performed and updated as necessary where a system change creates new privacy risks. Program offices and/or system owners should consult with the privacy team if they believe a project or system has changes that may create new privacy risks.[12]

DEFINITIONS[13]

Individual is a citizen of the United States or an alien lawfully admitted for permanent residence.

Information in identifiable form is information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

Information technology (IT), as defined in the Clinger-Cohen Act,[14] is any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

Major information system embraces "large" and "sensitive" information systems; as defined in OMB Circular A-130 (Section 6.u.) and annually in OMB Circular A-11 (section 300-4 (2003)), a system or project that requires special management attention because of its: (i) importance to the agency mission; (ii) high development, operating and maintenance costs; (iii) high risk, (iv) high return; and/or (v) significant role in the administration of an agency's programs, finances, property or other resources.

9-30-19

William D. Spencer
Senior Agency Official for Privacy

Date

[11] *See* OMB M-03-22 at Section II.E.
[12] OMB M-03-22 at Section II.B.b and c.: "Agencies must update their PIAs to reflect changed information collection authorities, business processes or other factors affecting the collection and handling of information in identifiable form."
[13] OMB M-03-22 at Section II.A.
[14] Clinger-Cohen Act of 1996, 40 U.S.C. § 11101(6).