PRIVACY PROGRAM PLAN

U.S. Merit Systems Protection Board

September 2023
(Version 1.0)

1. INTRODUCTION

1.1 Purpose

The purpose of the U.S. Merit Systems Protection Board's (MSPB or the Board) Privacy Program Plan is to provide an overview of MSPB's Privacy Program. The overview will provide information to MSPB, other Federal agencies, and the public regarding how MSPB implements and integrates privacy into the mission and programs at MSPB. This plan includes:

- a description of the structure of the Privacy Program;
- the resources dedicated to the Privacy Program;
- the role of the Senior Agency Official for Privacy (SAOP) and other privacy officials and staff;
- the strategic goals and objectives of the Privacy Program; and
- the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.[1]

1.2 Contact Information

You may visit MSPB's privacy webpage, located at www.mspb.gov/privacy, for more information regarding MSPB's Privacy Program, guidance, reports, and policy. Additionally, you may contact MSPB's Privacy Program at privacy@mspb.gov.

2. STRUCTURE OF THE PRIVACY PROGRAM

2.1 Mission Statement

It is the mission of MSPB's Privacy Program to protect the privacy of all individuals through compliance, training, and consultation. Among other activities, the Privacy Program implements requirements in the Privacy Act of 1974 (Privacy Act); E-Government Act of 2002 (E-Government Act); Federal Information Security Modernization Act (FISMA), as well as Office of Management and Budget (OMB) guidance and National Institute of Standards and Technology (NIST) best practices issued in furtherance of those Acts.

The Privacy Program adheres to the policy framework embodied in the Fair Information Practice Principles (FIPPs) to ensure that individual privacy is protected throughout the collection, maintenance, use, and dissemination of all personally identifiable information (PII) maintained by MSPB. PII is information which can be used to distinguish or trace an individual's identity such as their name, Social Security number (SSN), biometric records, etc., alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

---

[1] Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource* (OMB A-130) at Section 10, Paragraph 64, page 34.

The Privacy Program carries out the following core functions:

- Adjudicates requests for access and amendment in accordance with the Privacy Act;
- Develops and administers MSPB's privacy policies and procedures;
- Provides privacy awareness training and remediation training to MSPB personnel;
- Assesses new or proposed programs, systems, technologies, and business processes for privacy risks and provides recommendations to strengthen privacy protections;
- Collaborates with MSPB's Office of Information Resources Management (IRM) to implement and operationalize policies to secure the confidentiality, integrity, and availability of MSPB's information and information systems;
- Operates a data breach response program to ensure that all incidents involving PII are properly reported, investigated, and mitigated, as appropriate;
- Maintains updated privacy artifacts in compliance with legal requirements (e.g., System of Records Notices (SORN), Privacy Impact Assessments (PIA), and Privacy Act Notices);
- Coordinates Paperwork Reduction Act (PRA) efforts for new collections of information; and
- Provides consultation services to MSPB offices on privacy issues.

2.2 Privacy Program Organization

MSPB's Privacy Program operates as a program within the Office of the Clerk of the Board (OCB). OCB supports the Board's adjudication responsibilities by receiving and processing petitions for review and Federal employee appeals filed at MSPB headquarters, ruling on certain procedural matters, and issuing the Board's decisions. Additionally, OCB serves as MSPB's public information center, including providing information on the status of cases, distributing copies of Board decisions and publications, operating headquarters' library and online information services, and managing headquarters' subscriptions. OCB processes requests under the Privacy Act and the Freedom of Information Act (FOIA) and administers the agency's PRA and information management programs, including the Controlled Unclassified Information program and reporting related to Information Quality and Peer Review. Further, OCB certifies official records to the courts and Federal administrative agencies, manages MSPB's records systems, and manages the Government in the Sunshine Act program. Lastly, OCB initiates, maintains, and manages MSPB's legal research databases, public websites, and information publications, and prepares agency-level statistics in consultation with affected offices.

The main objectives of MSPB's Privacy Program are: to sustain privacy protections; minimize the agency's impact on the privacy of those we serve and with whom we work while balancing and supporting the agency in its mission; and to establish a culture of privacy awareness and compliance while supporting the agency in achieving its mission.

3. RESOURCES OF THE PRIVACY PROGRAM

MSPB's Privacy Program has dedicated personnel resources, including MSPB's Senior Agency Official for Privacy (SAOP), MSPB's Chief Privacy Officer (CPO), and a Government Information Specialist (Privacy Analyst).

4. THE ROLE OF THE SAOP, CPO, AND PRIVACY ANALYST

MSPB's SAOP, acting pursuant to OMB Memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy*, is designated by the Chairman of the Board. MSPB's SAOP ensures that the agency identifies and plans for the resources needed to implement its Privacy Program each year. To accomplish this mission, the SAOP has delegated privacy responsibilities to MSPB's CPO. The SAOP and CPO collaborate with members of MSPB's executive leadership team, including the Chief Information Officer, to review information technology (IT) capital investment plans and budgetary requests to ensure that privacy requirements and associated privacy controls are identified. The daily operations and all substantive components of MSPB's Privacy Program are led by the CPO and supported by the Privacy Analyst.

The CPO and Privacy Analyst collaborate with key stakeholders to ensure that privacy risks are addressed to the maximum extent possible, and work with contracting officials and program offices on solicitations to ensure that privacy considerations are addressed and included. Additionally, the CPO and Privacy Analyst have primary responsibilities over the agency's breach response, including the initial investigation, mitigation, and remediation measures required, if any.

4.1 Senior Agency Official for Privacy

The SAOP's primary responsibilities are to communicate MSPB's privacy vision, principles, and policies internally and externally, ensure all aspects of MSPB's Privacy Program are incorporated into MSPB's enterprise infrastructure, IT, and IT security program, and to support the CPO and Privacy Analyst in the implementation of MSPB's Privacy Program.

4.2 Chief Privacy Officer

The CPO manages the day-to-day responsibilities of MSPB's Privacy Program and reports directly to the SAOP on Privacy Program and compliance activities. The CPO is responsible for managing daily Privacy Program functions and possesses the requisite subject matter expertise to oversee agency privacy compliance activities and ensure the implementation of privacy policy and requirements. The CPO's responsibilities include:

- Serving as MSPB's senior authority on privacy policy, under supervision from the SAOP, on matters relating to the public disclosure of information, advising on privacy issues related to informed consent, disclosure risks, and data sharing;
- Developing and overseeing implementation of agency-wide policies and procedures relating to the Privacy Act, and assuring that personal information contained in Privacy Act systems of records is handled in compliance with its provisions;
- Managing privacy risks associated with MSPB activities that involve the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems;
- Advocating strategies for data and information collection and dissemination, to ensure MSPB's privacy policies and principles are reflected in all operations;

- Ensuring that MSPB employees have the appropriate training and education concerning privacy laws, regulations, policies, and procedures;
- Working with MSPB stakeholders to ensure the vendors with access to PII that engage in business with MSPB abide by Federal privacy requirements and that privacy considerations are incorporated into agency solicitations and procurements;
- Overseeing MSPB's process for reviewing and approving PIAs and Privacy Threshold Analyses (PTA) to ensure compliance with the E-Government Act;
- Overseeing MSPB's FISMA Assessment and Authorization process to ensure that new and existing IT systems appropriately address privacy-related risks;
- Providing governance and oversight of Privacy Program management and functions;
- Evaluating MSPB programs, systems, and initiatives for potential privacy implications to provide strategies to mitigate or reduce privacy risk in the risk management framework;
- Maintaining the agency's inventory of SORNs, drafting new and updating existing SORNs, and ensuring the MSPB SORN webpage is updated with current notices;
- Developing, approving, and submitting Privacy Act notices for submission to OMB and Congress and publication in the *Federal Register*;
- Maintaining and updating an inventory of PII that allows MSPB's Privacy Program to regularly review and reduce its PII to the minimum necessary while still allowing the performance of its authorized functions;
- Managing the MSPB Privacy Program webpage and providing information to the public on MSPB's privacy policies and practices to promote transparency and accountability;
- Providing information to MSPB employees on the agency's intranet Portal.
- Overseeing agency privacy incident reporting, response, notification, and remediation activities, maintaining a breach response plan, and conducting tabletop exercises to test breach response, the Breach Response Plan, procedures, and capabilities;
- Developing organizational metrics to evaluate success of the Privacy Program and ensure compliance with privacy laws, policies, and standards; and
- Developing and submitting privacy reports such as the annual SAOP FISMA report.

4.3 Privacy Analyst

The Privacy Analyst provides support for privacy projects and activities. The Privacy Analyst reports to the CPO and works closely on matters affecting MSPB's Privacy Program in its creation, collection, use, processing, storage, dissemination, disclosure, and disposal of information about individuals. The Privacy Analyst's responsibilities include:

- Gathering, monitoring, and evaluating all relevant information concerning systems collecting PII;
- Preparing, drafting, and reviewing privacy documentation (e.g., Privacy Program Plan, Breach Response Plan, privacy policies, SORNs, Privacy Act Statements, PTAs, and PIAs);
- Reviewing program-specific technological and administrative measures implemented to ensure the security of and data minimization within MSPB's IT systems;

- Responding to and mitigating suspected or confirmed privacy breaches and conducting follow-up activities to address any privacy vulnerabilities;
- Reviewing and applying subject matter expertise to MSPB policies, programs, projects, and initiatives to identify and mitigate privacy risks;
- Creating and compiling responsive information for the CPO, SAOP, and MSPB senior leadership on matters and inquiries related to MSPB's Privacy Program;
- Monitoring and analyzing legislative and policy proposals that could affect MSPB's Privacy Program and processes; and
- Collaborating with the CPO on privacy compliance issues and representing MSPB's Privacy Program at interagency meetings and conferences.

5. STRATEGIC GOALS AND OBJECTIVES FOR THE PRIVACY PROGRAM

GOAL 1

- **Conduct robust compliance and oversight programs to ensure adherence with Federal privacy and disclosure laws, regulations, guidance, and best practices.**

    - Objective 1.1 – Provide accountability and transparency in MSPB's privacy priorities and responsibilities by ensuring that MSPB is in compliance with the Privacy Act, the E-Government Act, OMB requirements, NIST privacy guidance, and best practices. This includes completing all the compliance activities and documentation, ensuring that MSPB's workforce is provided appropriate training, and providing guidance and interpretation to MSPB's stakeholders, including the Board, senior management, and regional and field offices in the application of Federal privacy laws, regulations, and best practices.

    - Objective 1.2 – Provide timely and efficient processing of requests for information and amendment under the Privacy Act.

    - Objective 1.3 – Review, assess, and advise MSPB staff with regard to agency programs, projects, information sharing arrangements, systems, and other initiatives in an effort to comply with the FIPPs, which includes limiting the collection, maintenance, use, and dissemination of PII whenever possible.

    - Objective 1.4 – Ensure that privacy-related breaches, complaints, and incidents at MSPB are reported systematically, efficiently processed, and appropriately mitigated and remediated in accordance with legal requirements and MSPB policies and procedures.

GOAL 2

- **Provide outreach, education, and training to promote a culture of privacy and transparency.**

    - Objective 2.1 – Provide guidance and implement policies related to privacy while collaborating with MSPB stakeholders to "bake-in" privacy at the beginning of initiatives, programs, projects, and systems, and ensure that privacy is considered throughout the lifecycle of each.

    - Objective 2.2 – Increase privacy awareness to MSPB personnel by fostering dialogue throughout the agency, providing targeted privacy training, and frequent outreach to ensure that MSPB offices are aware of the Privacy Program resources.

GOAL 3

- **Develop and maintain top privacy professionals in the Federal Government.**

    - Objective 3.1 – Support employee development and emphasize the importance of training and professional development in performance planning.

    - Objective 3.2 – Reward exceptional employee performance and recognize individual contributions which enhance the Privacy Program's mission.

GOAL 4

- **Establish metrics to track the effectiveness of MSPB's Privacy Program.**

    - Objective 4.1 – Identify areas of improvement based on past performance, operational experience, and external requirements.

6. PROGRAM MANAGEMENT AND PRIVACY CONTROL REQUIREMENTS.

6.1 Privacy Controls

MSPB's Privacy Program is in the process of formalizing certain baseline privacy controls, as contained in NIST Special Publication (SP) 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*. Privacy controls are selected and implemented under the leadership and oversight of the SAOP and CPO and in collaboration with IRM. A privacy control is an administrative, technical, or physical safeguard employed to ensure compliance with privacy requirements and manage privacy risks. Privacy controls may be common, system-specific, or hybrid.

The CPO updates policies, processes, and designations as necessary to ensure that privacy controls are implemented and remain effective to protect PII. System owners collaborate with the Privacy Program to select, implement, and assess privacy controls and monitor changes to systems that involve PII or present privacy risk. MSPB integrates privacy controls into the PIA.

6.2 Privacy Threshold Analysis (PTA)

A PTA is utilized at the earliest stages of the information lifecycle to help the Privacy Program identify privacy compliance requirements for activities that may have privacy implications and determine whether other privacy compliance documentation is required. A PTA is a questionnaire used to determine if a system contains PII, whether a PIA is required, whether a SORN is required, and if any other privacy requirements apply to the information system. MSPB completes PTAs when procuring a new IT system, when developing or significantly modifying an information system, or at the outset of any agency initiative that may involve PII.

The purpose of the PTA is to:

- Identify programs, projects, information collections, and information systems that are privacy-sensitive;
- Determine requirements for a PIA or additional privacy compliance requirements for the collection, maintenance, use, processing, sharing, or disposal of PII;
- Demonstrate that privacy considerations were included during the review of a program, project, information collection, or information system;
- Provide a record of the determination of privacy requirements for the program, project, collection, or information system for the program official, system owner, and the Privacy Program; and
- Demonstrate compliance with privacy laws, regulations, and policy.

6.3 Privacy Impact Assessment (PIA)

A PIA is required by Section 208 of the E-Government Act and analyzes how information in an identifiable form is collected, maintained, stored, and disseminated. The PIA analyzes the privacy risks as well as the protections and process for handling information to mitigate privacy risks. PIAs are conducted when:

1. Developing or procuring information systems or projects that collect, maintain, or disseminate information in an identifiable form, from or about, members of the public; or
2. Initiating a new electronic collection of information in identifiable form from 10 or more persons (excluding agencies, instrumentalities or employees of the Federal Government).

MSPB's PIAs, when drafted, describe: (1) the legal authority that permits the collection of information; (2) the specific type of information used by the system; (3) how and why the system uses the information; (4) whether the system provides notice to individuals that their information is used by the system; (5) the length of time the system retains information; (6) whether and with

whom the system disseminates information; (7) procedures individuals may use to access or amend information used by the system; and (8) physical, technical, and administrative safeguards applied to the system to secure the information.

6.4 System of Records Notices (SORN)

A system of records is a group of any records under the control of an agency from which information is retrieved by a unique identifier, including but not limited to an individual's name, SSN, symbol, or other identifier assigned to the individual. A Federal agency is not permitted to maintain a system of records without an associated SORN. MSPB adheres to Privacy Act requirements for publishing SORNs in the *Federal Register*. MSPB also publishes current SORNs on MSPB's privacy webpage.

6.5 Privacy Act Statements

Under the Privacy Act, agencies maintaining a system of records shall provide notice to the public at the time of collection of the information, the authority for the collection, the principal purpose for the use of the information collected, the routine uses for disclosure, and the effects of not providing the requested information. The Privacy Program collaborates with program stakeholders to meet this requirement.

6.6 Privacy Act Regulations

MSPB has promulgated regulations which implement the requirements contained in the Privacy Act. The regulations, located at 5 C.F.R. Part 1205, apply to all records maintained by MSPB that contain identifiable information about individuals and which are located as part of a system of records. MSPB's regulations establish, among other things, procedures that enable individuals to access records maintained about them; provide detailed procedures for how to amend inaccurate information; and limit who may access such information.

6.7 Contractors and Third Parties

MSPB's Privacy Program coordinates with agency contracting officials to ensure contractors and third parties that (1) create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII on behalf of the agency; or (2) operate or use information systems on behalf of the agency comply with the mandated privacy requirements. MSPB's Privacy Program coordinates with MSPB's Contracting Office to ensure that the applicable privacy clauses are included in the terms and conditions in contracts and other agreements involving the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of MSPB information.

6.8 Fair Information Practice Principles (FIPPs)

MSPB's Privacy Program adheres to the FIPPs. The FIPPs are a set of nine principles that are rooted in the tenets of the Privacy Act. The FIPPs form the basis of MSPB's privacy compliance policies and procedures governing the use of PII. The agency has incorporated the

following principles in several agency-wide processes to evaluate information systems, processes, programs, and activities that impact individual privacy. The FIPPs are:

- Access and Amendment – Individuals are provided with appropriate access to PII and the opportunity to correct or amend their PII.

- Accountability – MSPB monitors, audits, and documents compliance with the FIPPs through a number of processes, including but not limited to the PTA/PIA and SORN processes. Additionally, MSPB has incorporated key privacy requirements into the agency's Rules of Behavior, which are enforced through a process that can include discipline to strengthen accountability.

- Authority – MSPB creates, collects, uses, processes, stores, maintains, disseminates, and discloses PII if it has the authority to do so, and identifies this authority in the appropriate notice.

- Minimization – MSPB creates, collects, uses, processes, stores, maintains, disseminates, and discloses PII that is directly relevant and necessary to accomplish the legally authorized purpose. The PII is maintained for as long as is necessary to accomplish the purpose.

- Quality and Integrity – MSPB creates, collects, uses, processes, stores, maintains, disseminates, and discloses PII with the accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.

- Individual Participation – Individuals are involved in the process of using PII and, to the extent practicable, individual consent is granted for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Individuals may address concerns or complaints to MSPB's SAOP.

- Purpose Specification and Use Limitation – MSPB provides notice of the specific purposes for which PII is collected and only uses, processes, stores, maintains, disseminates, and discloses PII for the purpose explained in the notice.

- Security – MSPB ensures that administrative, technical, and physical safeguards are established to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, and disclosure.

- Transparency – MSPB provides clear and accessible notice regarding the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

7. PRIVACY RISK MANAGEMENT FRAMEWORK

MSPB adheres to the process described in NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations*, to incorporate information security and privacy risk management activities into the system development life cycle. The SAOP and CPO collaborate with MSPB's Chief Information Officer and Chief Information Security Officer to:

- Analyze data elements used by each of MSPB's information systems, including the information processed, maintained, and transmitted by each system, based on an impact analysis compliant with NIST FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*; and

- Conduct a PIA which assesses the privacy risks for each of MSPB's information systems.

8. OVERVIEW OF HANDLING AND PROTECTING PII

Handling and safeguarding PII maintained and used by MSPB is necessary to ensure the trust of MSPB's employees and stakeholders.

8.1. Recognizing PII

PII refers to information which 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, such as information relating to MSPB appellants. Sensitive PII is PII which if lost, compromised, or disclosed without authorization could result in harm, embarrassment, inconvenience, or unfairness to an individual.

It is always important to consider the context in which the information is used when determining the level of sensitivity of PII. The same types of information can be sensitive or non-sensitive depending on the context. For example, a list of employee names and phone numbers is less sensitive than a list of employee names and phone numbers who are subject to disciplinary action. The Privacy Program has procedures in place to analyze the sensitivity of PII and the harm its loss or publicity could potentially cause to affected individuals.

8.2. Minimizing the Collection of PII

MSPB complies with the Privacy Act's requirement to limit the collection of PII from individuals. MSPB maintains only relevant and necessary information about individuals, in accordance with a legally authorized purpose. MSPB also complies with OMB Circular A-130, *Managing Information as a Strategic Resource*, which directs agencies to eliminate unnecessary collections, maintenance, and use of SSNs.

MSPB's Privacy Program strives to coordinate with agency stakeholders to maintain an inventory of PII holdings and uses the PTA, PIA, and SORN processes to identify methods to further reduce the PII the agency collects and to ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely, and complete. Lastly, MSPB's SAOP and CPO ensures that MSPB minimizes the collection and use of PII in the context of MSPB forms and correspondence.

8.3. Handling and Transmitting PII

MSPB requires strict handling guidelines for employees and contractors who handle PII due to the nature of the data and the increased risk to an individual if data was to be compromised. Methods for handling PII include, but are not limited to the following, and must be done in accordance with MSPB's approved records schedules:

- Store sensitive PII on secure MSPB networks, systems, and MSPB-approved media;
- Secure sensitive paper PII by locking it in desks and filing cabinets;
- Remove visible PII from desks and office spaces when not in use (e.g., at the end of each day);
- Destroy sensitive PII by putting appropriate documents in MSPB shred bins;
- Delete sensitive electronic PII by emptying the computer's "recycle bin;"
- Only use MSPB-provided email addresses for conducting official business; and
- Encrypt sensitive PII on computers, media, and other devices, especially when sending data outside of MSPB's own information systems and provide passwords separately.

Sensitive PII may be distributed or released to other individuals only if authorized by the Privacy Act, MSPB's SORNs, and MSPB's regulations. Examples of authorized releases or sharing of sensitive PII include: (1) when it is necessary for MSPB personnel to complete work within the scope of the recipient's official duties; (2) the recipient has an official, job-based need to know; (3) the distribution is done in accordance with a legitimate underlying authority (e.g., a routine use in a SORN); and (4) sharing information is done in a secure manner. When in doubt, MSPB employees must treat PII as sensitive and must keep the transmission of sensitive PII to a minimum, even when it is protected by secure means.

Approved ways for communicating, sending, and receiving sensitive PII include:

- Fax – When faxing information, MSPB personnel should include a Privacy Act Cover Sheet (attached) to alert recipients about the contents and should notify the recipient before and after transmission.

- Mail – MSPB personnel should physically secure PII when in transit by sealing it in an opaque envelope or container, and mail it using a commercial service with tracking information. MSPB personnel should not mail or send sensitive PII by courier on MSPB-provided CDs, DVDs, hard drives, flash drives, USB drives, floppy disks, or other removable media unless the data is encrypted. Passwords should be sent separately.

- Hard Copy – All hard copy materials should be covered with a Privacy Act Cover Sheet (attached). MSPB personnel should hand-deliver documents containing sensitive PII whenever possible. MSPB personnel should not leave sensitive PII unattended on printers, fax machines, copiers, or in other common areas.

9. BREACH RESPONSE AND MANAGEMENT

MSPB has an obligation to protect the information of MSPB appellants, employees, and other stakeholders. The Privacy Program takes this obligation very seriously and has developed a policy and procedures to inform MSPB employees and contractors of their obligation to protect PII and to instruct them on specific steps they must take in the event there is an actual or potential compromise of PII. In accordance with OMB Memorandum 17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, and to safeguard PII, MSPB has established a Breach Response Plan. The Breach Response Plan informs MSPB employees and contractors of their responsibilities and obligations to protect PII, as well as defines standards for responding to suspected or confirmed breaches of PII and creates standards for compliance.

10. AWARENESS AND TRAINING

MSPB requires all employees and contractors with access to PII to complete privacy training when first beginning work with the agency and annually thereafter. The training provides an overview of important statutory, regulatory, and other Federal privacy requirements, including the Privacy Act and the E-Government Act.

10.1. New Employee Orientation Training

MSPB's Privacy Program provides live privacy training to all new employees upon onboarding. New employee orientation sessions provide an overview about the importance of privacy at MSPB, how to handle privacy-protected information, and the penalties for violating the Privacy Act.

10.2. Role-Based Training

In addition to new-hire and annual privacy training requirements, MSPB's Privacy Program looks for opportunities to provide role-based training to employees with specialized roles on a periodic basis, focusing on how employees in various MSPB offices should leverage the FIPPs as part of their official duties.

11. PRIVACY REPORTING

The FISMA requires Federal agencies to develop, document, and implement agency-wide information security programs that include plans and procedures to ensure the security of operations for information systems that support the operations of the agencies. All Federal agencies are required to submit an annual report to OMB, the United States Department of Homeland Security (DHS), specific Committees in the United States House of Representatives and the Senate, and the Government Accountability Office.

MSPB's Privacy Program completes the initial draft of the SAOP FISMA report, which is reviewed by the SAOP prior to submission. In response to questions developed by DHS and OMB, MSPB's SAOP FISMA report provides an overview of a variety of activities conducted by the Privacy Program during the reporting period.

12. CONCLUSION

MSPB is committed to safeguarding PII that MSPB appellants, agencies, employees, and other individuals entrust to the agency to carry out its statutory and administrative obligations. MSPB's Privacy Program uses all methods of regulation, policy, guidance, and principles to further this objective. Privacy considerations are embedded in all levels of decision-making and operations to continue to build a culture of privacy at MSPB.

WILLIAM SPENCER

Digitally signed by WILLIAM SPENCER
Date: 2023.09.28 13:58:08 -04'00'

William D. Spencer
Senior Agency Official for Privacy
September 28, 2023

PRIVACY DATA COVER SHEET

DOCUMENT(S) ENCLOSED MAY BE SUBJECT TO THE PRIVACY ACT OF 1974

WARNING

The enclosed document(s) shall not be accessed by, disclosed to, discussed with, or shared with individuals unless they have a direct need-to-know in the performance of their official duties. This/These document(s) shall be delivered directly to the intended recipient. DO NOT leave unattended or with an unauthorized individual.

Unauthorized disclosure of this information may result in PERSONAL LIABILITY with CIVIL and CRIMINAL penalties. 5 U.S.C. 552a(i) and (o).

When not under the continuing control and supervision of a person authorized to access this material, IT MUST BE, AT A MINIMUM, MAINTAINED UNDER LOCKED OR SECURED CONDITIONS.

If you believe that you have received this/these document(s) in error, please do not remove this cover sheet or otherwise access the document(s). Please immediately contact MSPB at the contact information below.

privacy@mspb.gov
202-653-7200