U.S. Merit Systems Protection Board

Information Resources Management Strategic Plan

FY 2026 - 2030

Introduction

A highly qualified Federal workforce managed under Merit System Principles (MSPs) and in a manner free from Prohibited Personnel Practices (PPPs) is critical to ensuring Federal agency performance and service to the public. MSPs are essential management practices that help ensure the Federal Government's ability to recruit, select, develop, maintain, and manage a high-quality workforce, and thereby reduce staffing costs and improve organizational results for the American people. PPPs are specific, proscribed behaviors that undermine MSPs and adversely impact the effectiveness and efficiency of the workforce and the Government. MSPB's fundamental function is to help ensure that the Federal workforce is managed in a manner consistent with MSPs and protected from PPPs.

This Information Resources Management (IRM) Strategic Plan was developed in accordance with 44 U.S.C. § 3506(b) and Office of Management and Budget Circular No. A-130, *Managing Information as a Strategic Resource*.

Background and Initiatives

The Merit Systems Protection Board (MSPB) recently completed an effort to modernize all enterprise business applications, telephony, and network infrastructure. We have offloaded as much maintenance burden as possible to service and cloud solutions. We have also moved software-defined networking and internet security to the cloud. Future projects include focusing on efficiencies gained by the implementation of additional business intelligence and pilot artificial intelligence (AI) systems.

Strategic Goals and Objectives

The following Strategic Goals and Objectives are based on MSPB's Strategic Plan for FY 2022-2026. They will be updated in FY 2026 as part of our updated Strategic Plan for FY 2026-2030.

Strategic Goal 1

Serve the public interest by protecting Merit System Principles and safeguarding the civil service from Prohibited Personnel Practices.

Objective	Supporting IRM Activities
Strategic Objective 1A-HQ: Provide understandable, high-quality resolution of HQ appeals, supported by fair and efficient adjudication and ADR processes.	• Case Management System (e-Appeal) • Cloud Productivity Tools • Business Intelligence

Strategic Objective 1B: Enforce timely compliance with MSPB decisions.	• Case Management System (e-Appeal) • Cloud Productivity Tools • Business Intelligence
Strategic Objective 1C: Conduct objective, timely studies of the Federal merit systems and Federal Human Capital (HC) management issues.	• Statistical Analysis Tools • Experience Management and Research Tools • Cloud Productivity Tools • AI • Business Intelligence
Strategic Objective 1D: Review and act upon the rules, regulations, and significant actions of OPM, as appropriate.	• Experience Management and Research Tools • Cloud Productivity Tools • AI • Business Intelligence

Strategic Goal 2

Advance the public interest through education and promotion of stronger merit systems, adherence to Merit System Principles, and prevention of Prohibited Personnel Practices.

Objective	Supporting IRM Activities
Strategic Objective 2A: Support and improve the practice of merit, adherence to MSPs, and prevention of PPPs in the workplace through successful, targeted outreach and engagement.	• Case Management System (e-Appeal) • Cloud Productivity Tools • AI • Business Intelligence
Strategic Objective 2B: Advance the understanding of merit, MSPs, and PPPs for stakeholders and the public by developing and sharing informational and educational materials and guidance.	• Experience Management and Research Tools • Cloud Productivity Tools • AI • Business Intelligence

Guiding Principles

Our technological purchases must be easy to maintain and low cost, and they must provide high value. Solutions must include a wide array of tools addressing the needs of multiple aspects of our business process. Wherever possible, we will utilize low- or no-code solutions. Public-facing tools must be intuitive, perform to standard acceptable levels, provide the public with the ability to manage and control their data, and protect user data from exposure.

Technology must reside in FedRAMP-compliant cloud environments. Data must be encrypted in transit and at rest. Backups will be performed regularly and kept in separate cloud locations.

Technology must be available 24/7, except for scheduled maintenance windows, and access must be independent of any physical office space.

MSPB technology must be easily scalable, and both technology and accompanying governance, policies, and procedures compliant to the highest possible level with the National Institute of Standards and Technology and the Federal Information Security Modernization Act standards.

Systems and data must be secure. Data must be continuously monitored, and mitigations must be automated. Logging must be in place. Access to any resource must require two-factor authentication.

Compliance

MSPB strives to comply with Section 508 of the Rehabilitation Act of 1973, as amended; FISMA; the Privacy Act of 1974; disaster recovery planning; Department of Homeland Security (DHS) continuous diagnostics and mitigation; and other directives from the Office of Management and Budget, DHS, and the President, including but not limited to the following:

- Executive Order 14306, *Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending EO 13694 and EO 14144* (June 6, 2025)
- Executive Order 14179, *Removing Barriers to American Leadership in Artificial Intelligence* (Jan. 23, 2025)
- Executive Order 14144, *Strengthening and Promoting Innovation in the Nation's Cybersecurity* (Jan. 16, 2025), as amended by EO 14306
- BOD-25-01, *Implementing Secure Practices for Cloud Services* (Dec. 17, 2024)
- M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (Jan. 26, 2022)
- BOD-22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities* (Nov. 3, 2021)
- BOD-18-01, *Enhance Email and Web Security* (Oct. 16, 2017)