U.S. Office of Personnel Management

Office of the Inspector General

Office of Audits

Final Audit Report

Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Benefits Plus System

Report Number 2023-ISAG-007
August 9, 2023

Executive Summary

Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Benefits Plus System

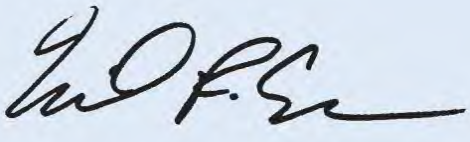
Report No. 2023-ISAG-007 **August 9, 2023**

Why Did We Conduct the Audit?

The Federal Information Security Modernization Act (FISMA) requires Inspectors General to complete annual evaluations of their respective agency's security programs and practices, which includes testing the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems. The Benefits Plus (BP) system was selected to include in this year's representative subset of systems because it is one of the Office of Personnel Management's (OPM) moderate risk, major systems, and an audit of its information technology (IT) security controls has not been performed within the past 10 years.

What Did We Audit?

The OPM Office of the Inspector General completed a performance audit of BP's IT security controls to ensure that they have been implemented in accordance with standards established by FISMA, the National Institute of Standards and Technology (NIST), and the OPM Office of the Chief Information Officer.



Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit of BP's IT security controls concluded that:

- BP's security categorization is compliant with NIST Special Publication (SP) 800-53, control RA-2 Security Categorization.
- We agree with BP's privacy threshold analysis conclusion that BP does not require a privacy impact assessment.
- BP's system security plan (SSP) includes numerous instances of outdated and inaccurate information.
- BP's SSP includes controls from NIST SP 800-53, Revision 4, which was withdrawn in September 2021.
- BP's security and risk assessments are compliant with NIST SP 800-53, control RA-3 Risk Assessment and CA-2 Control Assessments.
- BP's continuous monitoring control assessments are not consistently completed.
- BP's risk response for 9 out of 17 plans of action and milestones was not completed in accordance with organizational risk tolerance.
- BP has not been authorized to use 172 out of its 199 inherited controls.
- BP's business impact analysis does not document system component recovery priorities.
- BP's contingency plan test expired in August 2022.
- BP has vulnerable software in its IT environment.
- BP's control implementation documentation was inaccurate for 6 out of its 19 system-specific controls.

Abbreviations

ACC	**Agency Common Controls**
AO	**Authorizing Official**
ART	**Assessment Results Table**
ATO	**Authorization to Operate**
A&A	**Assessment and Authorization**
BIA	**Business Impact Analysis**
BP	**Benefits Plus System**
FIPS	**Federal Information Processing Standards**
FISMA	**Federal Information Security Modernization Act**
FY	**Fiscal Year**
GAGAS	**Generally Accepted Government Auditing Standards**
GRC	**Governance, Risk, and Compliance**
ISCM	**Information Security Continuous Monitoring**
ISSO	**Information System Security Officer**
IT	**Information Technology**
NIST	**National Institute of Standards and Technology**
OCIO	**Office of the Chief Information Officer**
OIG	**Office of the Inspector General**
OMB	**U.S. Office of Management and Budget**
OPM	**U.S. Office of Personnel Management**
PIA	**Privacy Impact Assessment**
P.L.	**Public Law**
POA&M	**Plan of Action and Milestones**
PTA	**Privacy Threshold Analysis**
Q	**Quarter**
RAR	**Risk Assessment Report**
RAT	**Risk Assessment Table**
SAP	**Security Assessment Plan**
SCM	**Security Controls Matrix**
SP	**Special Publication**
SSP	**System Security Plan**
U.S.	**United States**

Table of Contents

Report Fraud, Waste, and Mismanagement

I. Background

On December 17, 2002, the President of the United States (U.S.) signed Public Law (P.L.) 107-347, the E-Government Act, into law, which included Title III, the Federal Information Security Management Act. It requires (1) annual agency program reviews, (2) annual Inspector General (IG) evaluations, (3) agency reporting of the results of IG evaluations for unclassified systems to the U.S. Office of Management and Budget (OMB), and (4) an annual OMB report to Congress summarizing the material received from agencies.

In 2014, P.L. 113-283, the Federal Information Security Modernization Act (FISMA), was enacted and reaffirmed the objectives of the Federal Information Security Management Act. FISMA states that each year, each agency shall have an independent evaluation of its information security program and practices to determine their effectiveness. Evaluations shall include testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems. Agencies with an IG appointed under the Inspector General Act of 1978, as amended (5 U.S.C. §§ 401-424), shall have the evaluation performed by the IG of the agency or by an independent external auditor, as determined by the IG of the agency.

According to the Benefits Plus (BP) system security plan (SSP), BP is a data repository for Federal Employee Health Benefits Program and Federal Employee Dental and Vision Insurance Program information that is entered by the insurance provider and reviewed by the U.S. Office of Personnel Management (OPM). This information includes data regarding contract information, brochures, benefits, out-of-pocket limits and deductibles, plan codes, and member enrollment. BP serves as an information source for other OPM Healthcare and Insurance applications (Plan Comparison Tool and Brochure Creation Tool) and OPM.gov web pages for external and internal use.

BP has been included in this year's representative subset of systems to be evaluated because it is one of OPM's moderate risk, major systems, and an audit of its information technology (IT) security controls has not been performed within the past 10 years.

II. Objective, Scope, and Methodology

Objective

The objective of this audit was to determine if the OPM Office of the Chief Information Officer (OCIO) has implemented IT security controls for BP in accordance with standards established by FISMA, the National Institute of Standards and Technology (NIST), and the OPM OCIO.

Scope and Methodology

The scope of this audit included IT security controls defined by FISMA, NIST, and OPM OCIO policies, which impact the IT security posture of BP as of May 2023.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS), issued by the U.S. Comptroller General. GAGAS requires that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. Accordingly, the audit included an evaluation of related policies and procedures, control tests, and other auditing procedures we considered necessary to achieve our objective.

The audit objective was accomplished by reviewing the degree to which a variety of security program elements were implemented for BP, including:

- Security Categorization;
- Privacy Impact Assessment (PIA);
- System Security Plan (SSP);
- Security and Risk Assessments;
- Continuous Monitoring;
- Plan of Action and Milestones (POA&M);
- Authorization Memo;
- Contingency Planning;
- Vulnerability and Compliance Scanning; and
- NIST Special Publication (SP) 800-53, Revision 5, Security Controls.

Control tests were performed to determine the extent to which established controls and procedures are functioning as intended. NIST SP 800-53A, Revision 5, *Assessing Security and Privacy Controls in Information Systems and Organizations,* includes a comprehensive set of procedures for assessing the effectiveness of security and privacy controls defined in NIST SP

800-53, Revision 5. We used these potential assessment methods and artifacts, where appropriate, to evaluate BP's controls. This included interviews, observations, tests, and examination of computer-generated data and various documents including IT and other related organizational policies and procedures. Where appropriate, control tests utilized judgmental sampling methods. Results of judgmentally selected samples cannot be projected to the entire population since it is unlikely that the results are representative of the population as a whole.

In conducting the audit, we relied, to varying degrees, on computer-generated data. Due to time constraints, we did not verify the reliability of the data generated by the various information systems involved. However, nothing during this audit caused us to doubt the reliability of the computer-generated data used. We believe that the data was sufficient to achieve the audit objectives.

We considered BP's internal control structure in planning our audit procedures. These procedures were mainly substantive in nature, although we did gain an understanding of management procedures and controls to the extent necessary to achieve our audit objective. Since our audit would not necessarily disclose all significant matters in the internal control structure, we do not express an opinion on BP's internal controls taken as a whole.

The OPM Office of the Inspector General (OIG), as established by the Inspector General Act of 1978, as amended (5 U.S.C. §§ 401-424), performed the audit. The OPM OIG conducted the audit remotely from OPM's Jacksonville, Florida and Washington, D.C. offices between December 2022 and May 2023.

Compliance with Laws and Regulations

In conducting this audit, various laws, regulations, and industry standards were used as criteria to evaluate BP's control structure. These criteria included, but were not limited to, the following publications:

- E-Government Act of 2002 (P.L. 107-347), Title III, Federal Information Security Management Act of 2002;
- Federal Information Security Modernization Act of 2014 (P.L. 113-283);
- NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems;
- NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems;
- NIST SP 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations;
- NIST SP 800-39, Managing Information Security Risk;

- NIST SP 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations;
- Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems;
- FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems;
- OMB Circular A-130, Managing Information as a Strategic Resource;
- OMB Memorandum 04-04, E-Authentication Guidance for Federal Agencies; and
- OPM OCIO's IT security policies and procedures.

While generally compliant with respect to the items tested, OPM was not in compliance with all standards, as described in section III of this report, "Audit Findings and Recommendations."

III. Audit Findings and Recommendations

A. Security Categorization

BP's security categorization is adequate.

OMB Circular A-130, *Managing Information as a Strategic Resource*, requires Federal agencies to assign a security categorization to all Federal information and information systems. FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, defines standards to be used by Federal agencies to make security categorization decisions with the objective of providing sufficient information security controls according to risk. A system's minimum information security requirements are defined in FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, and are determined based on the security categorization it's assigned using FIPS Publication 199 guidance.

BP's security categorization document includes an analysis of the impact that will result from a loss of system and information confidentiality, availability, and integrity. OPM categorized BP as a "low" impact level for confidentiality and a "moderate" impact level for integrity and availability. In accordance with FIPS Publication 199, OPM used the maximum potential impact value to assign BP's overall security categorization as "moderate."

BP's security categorization is consistent with FIPS Publication 199 requirements. Additionally, the requirements of NIST SP 800-53, Revision 5, control RA-2 Security Categorization, have been adequately implemented.

No opportunities for improvement related to BP's security categorization were identified.

B. Privacy Impact Assessment

BP does not require a privacy impact assessment.

The E-Government Act of 2002 requires Federal agencies to perform a PIA for systems that collect, maintain, or disseminate information that is in an identifiable form. The PIA should address privacy related concerns including, but not limited to, what information is to be collected; why the information is being collected; with whom the information will be shared; and how the information will be secured. A privacy threshold analysis (PTA) documents the continuous monitoring of privacy risk and mitigation for the system and is used to determine whether a system requires a PIA.

BP's PTA was last updated in May 2021 and concluded that BP does not require a PIA because it is not designated as a privacy sensitive system. In accordance with OPM procedure, the PTA's designation was reviewed and reapproved by a designee of OPM's Chief Privacy Officer before the PTA's expiration date. Since BP is not a privacy sensitive system, the requirements of NIST

SP 800-53, Revision 5, control RA-8 Privacy Impact Assessments, have been adequately implemented.

No opportunities for improvement related to BP's PIA were identified.

C. System Security Plan

OMB Circular A-130 requires an SSP to be developed for all Federal information systems. SSPs document the security requirements of a system and describe the controls that are in place or planned to meet those requirements.

BP's SSP includes numerous instances of outdated and inaccurate information.

For Federal information systems to be granted an authorization to operate (ATO), a senior management official must accept the risks associated with the system. The decision to accept those risks should be based on an assessment of all the security controls that are applicable to the system. The SSP establishes and documents security controls for the system and is the basis for the authorization.

BP's SSP satisfies some of the requirements of NIST SP 800-53, Revision 5, control PL-2 System Security and Privacy Plans, including, but not limited to:

- Identifying individuals who fulfill system roles and responsibilities;
- Providing the security categorization and supporting rationale for the system; and
- Describing the mission and business processes supported by the system.

However, we identified the following opportunities for improvement related to BP's SSP.

1. System Security Plan Review

During our review of BP's SSP, we identified numerous instances of outdated and inaccurate information.

NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, states that "Once the information system security plan is developed, it is important to periodically assess the plan, review any change in system status, functionality, design, etc., and ensure that the plan continues to reflect the correct information about the system. … All plans should be reviewed and updated, if appropriate, at least annually."

OPM's *Security Planning Policy* states that OPM will implement NIST SP 800-53, Revision 4, control PL-2 System Security Plan, to review SSPs at least annually and ensure that they are approved by the authorizing official (AO) prior to implementation.

The most current version of BP's SSP was updated in November 2021. However, it was not

reviewed and approved by the AO. The last version of the SSP that was reviewed and approved by the AO was published in April 2020. Neither version of the SSP has been updated within the last year.

We identified the following specific weaknesses related to BP's implementation of NIST SP 800-53, Revision 5, control PL-2 System Security and Privacy Plans, which need to be addressed during the next update of BP's SSP.

- Control PL-2 states that the SSP "Explicitly [defines] constituent system components … ." However, BP's SSP includes a hardware inventory that is not accurate or complete. The inventory also states that servers are running an operating system that is not accurate.

- Control PL-2 states that the SSP "Include risk determinations for security and privacy architecture and design decisions … ." OMB Memorandum 04-04, *E-Authentication Guidance for Federal Agencies*, requires that agencies perform a risk assessment for electronic transactions performed by its systems to determine and then implement authentication processes that will provide the required level of assurance. Based on the assessment, each system is assigned an e-authentication assurance level (1 – 4) which represents the degree of certainty that a user has presented proper identification. BP's SSP documents the assurance level at 3, which does not match the assurance level 2 documented in the system's e-authentication risk assessment.

- Control PL-2 states that the SSP "Identify any relevant control baselines or overlays … ." According to the *OPM Security Authorization Guide*, "overlays are used during the control tailoring process to determine a viable set of security controls to provide the necessary protections to information systems." OPM's overlay includes a series of questions about the system that, when answered correctly, will produce a set of applicable controls. During our review of BP's overlay, we found that many questions were answered incorrectly including, but not limited to, what entity the system was owned by, what entity the system was managed by, and whether the system contained personally identifiable information.

- Control PL-2 states that the SSP "Describe the controls in place or planned for meeting the security and privacy requirements … ." In the past, OPM used a document called a security controls matrix (SCM) to capture this information. However, OPM has recently started tracking this information in its governance, risk, and compliance (GRC) application as well as the SCM. When comparing the information in the SCM and GRC, we found many discrepancies between the two sources of information. The control type and implementation for 12 out of 13 controls that are categorized as "not applicable" in the SCM do not match documentation in the GRC application. Furthermore, the control type and implementation for 48 out of 61 controls that are categorized as "planned" in the SCM do not match documentation in the GRC application.

Failure to maintain a current and accurate SSP negatively impacts OPM's ability to ensure that the security and privacy requirements of the system are met.

Recommendation 1:

We recommend that OPM review and update BP's SSP to correct all issues identified during this audit.

OPM's Response:

"Concur. OPM will update BP's SSP to resolve the discrepancies between the security controls matrix (SCM) and the governance, risk, and compliance (GRC) and request AO review and approval of the SSP."

OPM OIG Comment:

As part of the audit resolution process, OPM's OCIO should provide OPM's Internal Oversight and Compliance office with evidence that this recommendation has been implemented. This statement also applies to all subsequent recommendations in this audit report that OPM agrees to implement.

2. Withdrawn Controls

During our review of BP's SSP, we identified that the controls documented in the SSP, which have been selected and implemented to meet the system's security requirements, are based on a publication of NIST SP 800-53 that was withdrawn in September 2021.

OMB's revised Circular A-130 requires that Federal agencies "Employ a process to select and implement security controls for information systems and the environments in which those systems operate that satisfies the minimum information security requirements in FIPS Publication 200 and security control baselines in NIST SP 800-53, tailored as appropriate … ." This process was last performed for BP using NIST SP 800-53, Revision 4, but has not been reperformed to reflect the revisions included in NIST SP 800-53, Revision 5, which was published in September 2020.

OMB's revised Circular A-130 states that "For legacy information systems, agencies are expected to meet the requirements of, and be in compliance with, NIST standards and guidelines within one year of their respective publication dates unless otherwise directed by OMB."

Failure to select and implement current versions of NIST SP 800-53 security controls increases the risk that the system will not be compliant with minimum information security requirements defined in FIPS Publication 200.

Recommendation 2:

We recommend that OPM update BP's SSP to include NIST 800-53, Revision 5, controls that have been selected and implemented to meet the system's security requirements.

OPM's Response:

"Concur. OPM will update BP's SSP to address NIST 800-53, Revision 5."

D. Security and Risk Assessments

BP's security and risk assessments are adequate.

OMB Circular A-130 requires that Federal agencies "Conduct and document assessments of all selected and implemented security and privacy controls to determine whether security and privacy controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable requirements and to manage security and privacy risks … ." For the AO to grant a system an ATO, the AO must receive essential information about the security posture of the system which includes security control assessment results.

According to the *OPM Security Authorization Guide*, the security assessment plan (SAP) describes a security assessment's scope and procedures. Using the SAP, an assessment of the system's implemented security controls will be performed. The results of the assessment will be included in the assessment results table (ART). Using the ART, the Information System Security Officer (ISSO) documents a risk assessment for all identified weaknesses in a risk assessment table (RAT). All the residual risks remaining in the system are summarized in a risk assessment report (RAR) which is presented to the AO to review before making an authorization decision.

OPM tests all of a system's applicable controls over a three-year period. A subset of controls are tested triennially during an independent security controls assessment. The remaining controls are tested as part of the system's continuous monitoring activities.

BP's most recent SAP was for an independent security controls assessment performed from March 2020 to April 2020. The results were documented in an ART and a risk assessment of identified weaknesses was documented in a RAT. The residual risks remaining in the system were captured in a RAR and shared with BP's AO. We also reviewed continuous monitoring activities completed within the triennial period and verified that an acceptable portion of the system's applicable controls were tested.

All requirements of NIST SP 800-53, Revision 5, control CA-2 Control Assessments and RA-2 Risk Assessment have been adequately implemented by BP's security and risk assessments.

No opportunities for improvement related to BP's security and risk assessments were identified.

E. Continuous Monitoring

BP's continuous monitoring control assessments are not consistently completed.

OMB Circular A-130 requires Federal agencies to develop and implement an information security continuous monitoring (ISCM) strategy. ISCM is the maintenance of ongoing awareness of information security, vulnerabilities, and threats to support an agency's ability to manage risk. The ISCM strategy must define the degree of rigor and the frequency at which all controls selected to implement for the system are evaluated.

According to NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations*, a system-level ISCM strategy addresses monitoring for controls that are not covered by the organization-level continuous monitoring strategy. According to *OPM Continuous Monitoring and Ongoing Authorization Strategy*, information systems inherit the assessment results performed on controls that are fully inherited from provider systems (i.e., inherited controls and agency common controls) and portions of controls that are partially inherited from provider systems (i.e., hybrid controls). It is the responsibility of the system's ISSO to assess controls that are fully implemented by the system (i.e., system-specific controls) and system-specific portions of hybrid controls.

We reviewed BP's ISCM documentation from quarter (Q) 2 of fiscal year (FY) 2022 to Q1 of FY 2023 and determined that it satisfies some requirements of NIST SP 800-53, Revision 5, control CA-7 Continuous Monitoring, including, but not limited to:

- Established system-level metrics to be monitored;
- Response actions to address assessment results; and
- Routine reporting of the security and privacy status of the system to necessary personnel.

However, we identified the following opportunity for improvement related to BP's ISCM.

1. Ongoing Control Assessments

During our review of BP's ISCM documentation, we identified that OPM did not complete all ongoing security control assessments scheduled during Q1 of FY 2023.

BP's ATO was granted in December 2021, contingent upon BP's participation in ISCM. We received evidence of full participation during FY 2022. However, BP did not complete all ongoing security control assessments scheduled during Q1 of FY 2023 in accordance with ISCM strategy. At the end of Q1 of FY 2023, assessments for 9 out of 74 hybrid and system-specific controls were overdue. The lapse in ISCM had been previously identified by OPM and a POA&M was created in December 2022 to remediate the weakness. OPM was on track to resolve the POA&M by completing all ongoing security control assessments

scheduled during Q2 of FY 2023, but OPM failed to complete assessments scheduled during March 2023.

OPM's *Continuous Monitoring Policy* states that OPM will implement NIST SP 800-53, Revision 4, control CA-7 Continuous Monitoring, to "[implement] a continuous monitoring program that includes … Ongoing security control assessments in accordance with the organizational continuous monitoring strategy."

Failure to perform ISCM activities negatively affects OPM's ability to maintain ongoing awareness of information security, vulnerabilities, and threats in order to support organizational risk management decisions.

Recommendation 3:

We recommend that OPM complete all scheduled ongoing security control assessments for an entire quarter.

OPM's Response:

"Concur. OPM will complete 3 consecutive months of assessments at the end of June 2023 and will provide documentation to OIG."

F. Plans of Action and Milestones

A POA&M is an action plan used by Federal agencies to describe steps that will be taken to remediate control weaknesses that are identified during control assessments, audits, and continuous monitoring. POA&Ms define resource requirements, milestones, and timelines.

The risk response for 9 out of 17 open POA&Ms was not performed in accordance with organizational risk tolerance.

OPM has implemented agencywide POA&M procedures to track known IT security weaknesses associated with the agency's information systems. In order for a system to receive an ATO, the AO must accept the risks associated with a system's control weaknesses or require that they are remediated first. POA&Ms are included in a system's authorization documentation so that the AO can ensure that there is agreement on the steps that should be taken to remediate all risks, prior to granting an ATO.

We reviewed all of BP's POA&Ms from Q2 of FY 2022 through Q2 of FY 2023 and identified the following opportunity for improvement.

1. Untimely POA&Ms

During our review of BP's POA&Ms, we identified that the risk response for 9 out of 17 open POA&Ms was not performed in accordance with organizational risk tolerance.

The authorization memo is the official letter granting a system an ATO based on whether the organization's risk tolerance will accommodate the risks documented in the system's RAR and the planned risk response actions documented in the system's POA&Ms. BP's ATO was granted in December 2021, contingent upon the submission of evidence demonstrating the completion of each POA&M milestone within 60 days of the ATO for moderate risk POA&Ms and 120 days of the ATO for low risk POA&Ms. Additionally, OPM's *Information Technology Security FISMA Procedures* state that "The program offices shall establish a reasonable timetable for resolution or mitigation of the POA&M items, not to exceed one-calendar year from discovery." BP has seven moderate risk POA&Ms and two low risk POA&Ms that have not satisfied either requirement.

NIST SP 800-53, Revision 5, control RA-7 Risk Response, states that the organization "Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance."

NIST SP 800-39 states that "Risk response strategies specify: (i) individuals or organizational subcomponents that are responsible for the selected risk response measures and specifications of effectiveness criteria (i.e., articulation of indicators and thresholds against which the effectiveness of risk response measures can be judged); (ii) dependencies of the selected risk response measures on other risk response measures; (iii) dependencies of selected risk response measures on other factors (e.g., implementation of other planned information technology measures); (iv) implementation timeline for risk responses; (v) plans for monitoring the effectiveness of the risk response measures; (vi) identification of risk monitoring triggers; and (vii) interim risk response measures selected for implementation, if appropriate."

Failure to respond to findings in accordance with organizational risk tolerance leaves the organization vulnerable to a higher level of risk than it has determined to be acceptable.

Recommendation 4:

We recommend that OPM reevaluate the risk response strategy for the untimely POA&Ms identified during this audit, in accordance with organizational risk tolerance.

OPM's Response:

"Concur. OPM is committed to addressing findings in accordance with organizational risk tolerance. We will follow OPM's policy related to risk tolerance and monitoring POA&Ms."

Recommendation 5:

We recommend that OPM complete the untimely POA&Ms identified during this audit, in accordance with risk response activities defined by OPM in response to Recommendation 4.

OPM's Response:

"Concur. OPM is committed to addressing findings in accordance with organizational risk tolerance. We will update POA&Ms for BP to comply with OPM's organizational risk tolerance."

G. Authorization Memo

OMB Circular A-130 requires all Federal information systems to have a valid authorization. An authorization memo is an official management decision to authorize a system to operate and accept its known risks.

BP has not been authorized to use 172 of its 199 inherited controls.

Previously, OMB required Federal information systems to be routinely reauthorized in accordance with agency risk tolerance, but Federal agencies now have the option to continuously monitor their systems to fulfill the authorization requirement. OPM does not yet have a mature program in place to continuously monitor system security controls. Therefore, OPM systems are required to be routinely reauthorized in accordance with agency risk tolerance, which OPM has defined as at least once every three years.

BP received an ATO in December 2021. The authorization is valid until December 2023 and is contingent upon maintenance and/or completion of various security-related tasks specified in the authorization memo. These tasks include, but are not limited to, participation in continuous monitoring and timely remediation of POA&Ms, both of which have weaknesses that were identified during this audit and are discussed in the "Plan of Action and Milestones" and "Continuous Monitoring" sections of this report, respectively. The authorization memo states that at the end of this authorization period, the status of all required security-related tasks defined in the memo will be reviewed and the results will directly impact subsequent authorization recommendations for BP.

BP's authorization memo satisfies some of the requirements of NIST SP 800-53, Revision 5, control CA-6 Authorization, including, but not limited to:

- A senior official is assigned as the AO for the system;
- The AO has authorized the system to operate; and
- The ATO has been routinely updated according to policy.

However, we identified the following opportunity for improvement related to BP's authorization memo.

1. Unauthorized Inherited Controls

We reviewed all security controls that BP has selected to inherit from the agency or provider systems. Out of the 199 inherited controls, which includes agency common controls, the provider systems' AO has not authorized BP to subscribe to 172 of them.

BP's ISSO submitted a request to inherit controls from provider systems in January of 2023, but the request had not been approved by the end of our fieldwork. An AO has not been assigned to handle the request for 150 out of the 172 controls that are pending authorization for BP to inherit.

NIST SP 800-53, Revision 5, control CA-6 Authorization, states that the organization "Assign a senior official as the [AO] for common controls available for inheritance by organizational systems [and]… Ensure that the [AO] for common controls authorizes the use of those controls for inheritance by organizational systems … ."

Failure to ensure that senior officials are authorizing the use of inheritable controls increases the risk that subscriber systems will not be appropriately protected by provider system controls.

Recommendation 6:

We recommend that OPM assign a senior official as the AO responsible for authorizing the use of inherited and common controls.

OPM's Response:

"Concur. OPM is finalizing the Assessment & Authorization (A&A) package for the Agency Common Controls (ACC) program. The A&A package will identify the AO."

OPM OIG Comment:

Finalizing the Assessment and Authorization (A&A) package for the Agency Common Controls (ACC) program will demonstrate significant progress toward implementing this recommendation. However, this recommendation must be implemented for all systems that provide inheritable controls, not just controls provided by the agency.

Recommendation 7:

We recommend that OPM ensure that the AO for inherited and common controls that BP has selected to inherit authorizes BP to inherit those controls.

OPM's Response:

"Concur. OPM is finalizing the A&A package for the Agency Common Controls (ACC) program. The AO will authorize the inherited controls."

OPM OIG Comment:

Finalizing the A&A package for the ACC program will demonstrate significant progress toward implementing this recommendation. However, this recommendation must be implemented for all systems that provide inheritable controls, not just controls provided by the agency.

H. Contingency Planning

OMB Circular A-130 requires that Federal agencies develop and test contingency plans for all of their information systems. Contingency planning refers to policies, procedures, and techniques employed to proactively define and prepare a response to recover information systems in the event of a service impacting incident.

BP's contingency plan has not been tested since August 2021.

OMB Circular A-130 requires that contingency plans for Federal information systems identify essential missions and business functions and associated contingency requirements. This is accomplished by performing a business impact analysis (BIA), which is a key component of the contingency planning process. The purpose of the BIA is to correlate the system with the mission and business processes that it supports and use that information to describe the consequences of a service impacting incident affecting the system.

BP's contingency plan satisfies some of the requirements of NIST SP 800-53, Revision 5, control CP-2 Contingency Plan, including, but not limited to:

- Contingency requirements for essential mission and business functions are identified;
- Individuals are assigned with defined contingency roles and responsibilities; and
- Continuity of essential mission and business functions is addressed.

However, we identified the following opportunities for improvement related to BP's contingency planning controls.

1. Contingency Plan Review

Initially, OPM provided a contingency plan that had not been reviewed and updated since October 2021.

OPM's *Contingency Planning Policy* states that OPM will implement NIST SP 800-53, Revision 4, control CP-2 Contingency Planning, to "Review the contingency plan for the information system at [least annually] [and] … Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing." OPM had previously identified that BP's contingency plan had expired in October 2022 and already opened a POA&M to remediate the weakness.

Prior to the end of this audit, OPM remediated this weakness by producing an updated contingency plan that was reviewed and approved as of April 2023. Therefore, we will not issue a recommendation for this finding.

2. Business Impact Analysis

During our review of BP's BIA, we identified that recovery priorities for system components are not documented.

NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, states that the three steps typically involved in accomplishing a BIA are to determine mission and business processes and criticality; identify resources required for recovery; and identify recovery priorities for system resources. NIST clarifies that system resources include "facilities, personnel, equipment, software, data files, system components, and vital records." OPM's contingency planning documentation includes recovery priorities for some system resources but not system components.

OPM's *Contingency Planning Policy* states that OPM will implement NIST SP 800-53, Revision 4, control CP-2 Contingency Plan, to "Develop a contingency plan for the system that … Provides recovery objectives, restoration priorities, and metrics … ." Additionally, FISMA requires that "System level BIAs [include] … identification of recovery priorities for system resources," which includes system components.

Failure to document recovery priorities for system components increases the risk that mission/business processes will not be restored within their maximum tolerable downtimes.

Recommendation 8:

We recommend that OPM identify and document recovery priorities for BP's system components in BP's BIA.

OPM's Response:

"Concur. The BP BIA was updated May 17, 2023 with recovery priorities based on NIST 800-53, Revision 5. OPM notified OIG that the updated version of the BIA is in the A&A package."

OPM OIG Comment:

In response to the draft audit report, OPM provided an updated BIA. However, in terms of content, the updated BIA is identical to the original BIA assessed during our audit. The updated BIA does not identify and document recovery priorities for BP's system components and so it does not satisfy the intent of the recommendation.

3. Contingency Plan Testing

During our review of BP's most recent contingency plan test, we identified that contingency plan testing is not being completed annually in accordance with OPM policy.

The last contingency plan test was performed in August 2021. OPM was unable to perform a contingency plan test for BP during 2022 because the system was being migrated to a new environment. A POA&M was created in August 2022 and included plans to remediate the weakness by performing a contingency plan test in March 2023. However, this test was not performed.

OPM's *Contingency Planning Policy* states that OPM will implement NIST SP 800-53, Revision 4, control CP-4 Contingency Plan Testing, to "Test the contingency plan for the information system [at least annually] … ."

Failure to routinely perform contingency plan testing increases the risk that OPM will be unable to meet recovery objectives in the event of a service impacting incident.

Recommendation 9:

We recommend that OPM perform a test of BP's contingency plan.

OPM's Response:

"Concur. OPM completed a test of BP's contingency plan on June 1, 2023. OPM will provide the test evidence to OIG under separate cover."

I. Vulnerability and Compliance Scanning

BP has vulnerable software in its environment.

NIST SP 800-53A, Revision 5, *Assessing Security and Privacy Controls in Information Systems and Organizations*, states that an examination of vulnerability scanning results and configuration settings can be performed to assess the implementation of vulnerability and configuration management controls. Accordingly, we judgmentally selected a sample of servers to include in vulnerability and compliance scans which OPM performed on our behalf. Out of the 43 servers within BP's system boundary, we included all 16 servers in BP's user acceptance testing

environment. Our sample selection was based on OPM's attestation that BP's user acceptance testing environment has the same controls as the production environment. This allowed us to perform our test without interfering with production server operations.

We also performed an examination of historical vulnerability scan results from BP's web application.

We identified the following opportunities for improvement related to BP's vulnerability and configuration management controls.

1. Web Application Scanning

Initially, OPM informed us that BP's web application was not included in routine web application scanning but there was an ongoing project to include it in the future.

OPM's *Patch and Vulnerability Management Polic*y states that OPM will implement NIST SP 800-53, Revision 4, control RA-5 Vulnerability Monitoring and Scanning, to "Scan for vulnerabilities in the information system and hosted applications [at least monthly] and when new vulnerabilities potentially affecting the system/applications are identified and reported."

Prior to the end of this audit, OPM resolved this weakness by successfully completing the project to include BP in routine web application scanning and performing scans in May 2023. Therefore, we will not issue a recommendation for this finding.

2. Unsecure Configurations

As a result of our vulnerability scanning exercise and an examination of results from a historical web application scan, we identified that multiple BP servers and the web application have one or more high-risk unsecure configurations.

The unsecure server configuration identified during our vulnerability scanning exercise had been previously identified by OPM, and a POA&M was created in January 2020 to remediate the weakness. According to the POA&M, the unsecure configuration has been corrected as of December 2022, and the POA&M is awaiting review for closure. The POA&M was scheduled to be completed by January 2023. However, the unsecure configuration was still identified by our vulnerability scan in February 2023.

The historical web application scan results for BP included two high-risk unsecure web application configurations. OPM has a POA&M that was opened in June 2020 to track the remediation of one of the unsecure configurations. According to the POA&M and information from the web application scan, this vulnerability is caused by a lack of input validation. The POA&M states that a plan to implement input validation was created as of March 2023. The POA&M was scheduled to be completed by April 2023. A POA&M for the second unsecure web application configuration has not been created.

OPM's *Patch and Vulnerability Management Policy* states that OPM will implement NIST SP 800-53, Revision 4, control RA-5 Vulnerability Monitoring and Scanning, to "Remediate legitimate vulnerabilities [using OPM Plan of Action and Milestones procedures] in accordance with an organizational assessment of risk."

OPM's *System and Information Integrity Policy* states that OPM will implement NIST SP 800-53, Revision 4, control SI-10 Information Input Validation, to "Configure the information system to check the validity of [internal and external information inputs]."

Failure to remediate legitimate vulnerabilities in a timely manner in accordance with an organizational assessment of risk leaves systems susceptible to exploits which leverage those vulnerabilities.

Recommendation 10:

We recommend that OPM remediate unsecure configurations identified during this audit using OPM's plan of action and milestones procedures in accordance with an organizational assessment of risk for all affected BP servers and the web application.

OPM's Response:

"Concur. Using OPM's plan of action and milestones procedure, OPM is currently remediating identified unsecure configurations for affected BP servers and web application."

Recommendation 11:

We recommend that OPM configure BP's web application to check the validity of internal and external information inputs.

OPM's Response:

"Partially Concur. The text entered in BP is checked by the web application firewall. OPM will review the web application configuration to identify further checks of the validity of information inputs."

OPM OIG Comment:

This finding is based on web application vulnerability scan results which stated that one of the vulnerabilities could be resolved by improving input validation. Additionally, OPM has an existing POA&M tracking the remediation of a previously identified weakness related to input validation. If OPM has implemented a web application firewall that remediates the vulnerabilities included in the web application vulnerability scan and OPM's POA&M, please provide OPM's Internal Oversight and Compliance office with this evidence.

Furthermore, OPM's *System and Information Integrity Policy* states that OPM will implement NIST SP 800-53, Revision 4, control SI-10 Information Input Validation, to "Configure the information system to check the validity of internal and external information inputs." When submitting evidence, please consider that the web application firewall may only be able to validate external information inputs. Different mechanisms may be needed to comply with OPM's policy which requires validation of internal information inputs.

3. Unsupported Software

As a result of our vulnerability scanning exercise, we identified that multiple BP servers have unsupported software.

In response to this finding, OPM stated that it removed one of the versions of unsupported software but was unable to validate the presence of the second version of unsupported software. We requested evidence of any documented remediation efforts (e.g., projects or roadmaps, etc.). However, we only received a written attestation that the vulnerabilities were remediated. No additional evidence was provided demonstrating that the unsupported software was removed or that our scan result was a false positive.

NIST SP 800-53, Revision 5, control SA-22 Unsupported System Components, states that the organization "Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or … [acquire] alternative sources for continued support … ."

Failure to remove unsupported software from the IT environment increases the risk that components which are no longer receiving critical security patches could be compromised.

Recommendation 12:

We recommend that OPM replace or identify extended support for unsupported software identified during this audit for all affected BP servers.

OPM's Response:

"Concur. OPM will remediate unsupported software by upgrading to supported versions of the software."

4. Missing Patches

As a result of our vulnerability scanning exercise, we identified multiple BP servers with a security-relevant software update that has not been installed within 30 days of its release, in accordance with OPM policy.

According to historical vulnerability scan results, the missing security-relevant software update was first discovered by OPM in August 2022. However, the update has a publication date of December 2019. In response to this finding, OPM stated that the patch cannot be installed until another upgrade is performed. OPM provided documentation suggesting that a POA&M had been created to track the remediation of this vulnerability. However, this POA&M has not been created.

OPM's *Patch and Vulnerability Management Policy* states that OPM will implement NIST SP 800-53, Revision 4, control SI-2 Flaw Remediation, to "Install security-relevant software and firmware updates within [30 days] of the release of the updates."

Failure to install security-relevant software updates within the organization-defined period after their release increases the risk that vulnerable systems could be compromised.

Recommendation 13:

We recommend that OPM install the security-relevant software update identified during this audit for all affected BP servers.

OPM's Response:

"Concur. OPM will install the security-relevant software update identified for affected BP servers."

5. Configuration Settings

As a result of our compliance scanning exercise, we identified multiple BP servers with configurations that are not compliant with OPM's established configuration settings.

In response to this finding, OPM stated that it was not previously aware of the non-compliant configurations because the established configuration settings had been recently developed in January 2023. The first compliance scan using the newly established configuration settings was performed in March 2023. OPM stated that it will be creating a POA&M to track the remediation of non-compliant configuration settings. However, this POA&M has not been created.

OPM's *Secure Configuration Management Policy* states that OPM will implement NIST SP 800-53, Revision 4, control CM-6 Configuration Settings, to "Implement the configuration settings [and] … Identify, document, and approve any deviations from established configuration settings for all configurable devices based on compelling business requirements."

Failure to implement established configuration settings and identify, document, and approve deviations from those settings increases the risk that systems could have unsecure configurations.

Recommendation 14:

We recommend that OPM review all BP servers for non-complaint configurations identified during this audit and either correct non-compliant configurations or document and approve deviations with a compelling business requirement.

OPM's Response:

"Concur. OPM will review the identified BP servers and will either correct the configuration or document and approve the deviation with the business requirement."

J. NIST SP 800-53 Controls Testing

NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, provides guidance for implementing a variety of security controls for information systems supporting the Federal government.

BP adequately implemented 16 of the 33 controls tested.

Out of a total of 275 NIST SP 800-53, Revision 5, controls that are applicable to BP, we judgmentally selected a sample of 33 to test. Our judgmental sample was selected from high-risk areas identified during the planning phase of this audit and includes controls related to system authorization documentation; vulnerability and configuration management; and all controls that are fully implemented by the system (i.e., system-specific controls). One or more controls from each of the following control families were tested:

- Assessment, Authorization, and Monitoring;
- Configuration Management;
- Contingency Planning;
- Identification and Authentication;
- Risk Assessment;
- Planning;
- System and Services Acquisition; and
- System and Information Integrity.

Our tests concluded that 16 out of the 33 controls assessed during this audit have been adequately implemented. Opportunities for improvement that have not been captured in the preceding sections are detailed in the following sections.

1. Control Documentation

During our review of BP's system-specific controls, we identified that documentation did not accurately describe the implementation of 6 out of the 19 controls.

To test the effectiveness of system-specific controls, we requested evidence of each control's implementation based on what was described in BP's control documentation. In response, OPM provided updated control documentation which changed the categorization of six controls from system-specific to hybrid or inherited and altered the description of the control. Due to these changes, some of our controls testing was inconclusive.

NIST SP 800-53, Revision 5, control PL-2 System Security and Privacy Plans, states that the organization "Develop security and privacy plans for the system that … Describe the controls in place or planned for meeting the security and privacy requirements … ." NIST elaborates further, stating that SSPs "describe the intended application of each selected control in the context of the system with a sufficient level of detail to correctly implement the control and to subsequently assess the effectiveness of the control."

Failure to correctly categorize controls and describe their implementation with sufficient detail increases the risk that controls may not be sufficiently applied and monitored for effectiveness.

Recommendation 15:

We recommend that OPM perform a review of all BP's controls to ensure that all controls have the correct control type, and the implementation of each control is described with sufficient detail.

OPM's Response:

"Concur. OPM will review control types and document with sufficient implementation detail to ensure the SSP is compliant with NIST 800-53, Revision 5."

2. Error Handling

OPM has not demonstrated that BP generates helpful error messages that are only viewable to defined personnel and do not reveal sensitive information about the system.

OPM's description of the control implementation states that "Friendly error messages are displayed which do not provide any information that could be exploited." However, a POA&M has been open since June 2020 to track the remediation of a weakness related to this control. When asked to explain the identified weakness and clarify how the POA&M will remediate the weakness, OPM did not provide a relevant response.

NIST SP 800-53, Revision 5, control SI-11 Error Handling, states that the system "Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited [and] … Reveal error messages only to [organization-defined personnel or roles]."

Failure to appropriately control the content of error messages and who can view them increases the risk that exploitable information about the system could be exposed to unauthorized users.

Recommendation 16:

We recommend that OPM update BP to generate helpful error messages that are only viewable to defined personnel and do not reveal sensitive information about the system.

OPM's Response:

"Concur. OPM will update and remediate the associated POA&M. We will thereafter provide evidence to OIG to close this recommendation."

Appendix

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

July 6, 2023

Memorandum for: Eric Keehan
Office of the Inspector General (OIG)
Chief, Information Systems Audits Group

From: Laurie Bodenheimer
Associate Director, Healthcare and Insurance

CHERYL DAMMONS Digitally signed by CHERYL DAMMONS Date: 2023.07.06 08:27:23 -04'00'

Through: Guy Cavallo
Chief Information Officer

GUY CAVALLO Digitally signed by GUY CAVALLO Date: 2023.07.06 14:41:05 -04'00'

Subject: Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Benefits Plus System – FY 2023, (Report No. 2023-ISAG-007)

Thank you for providing OPM the opportunity to respond to the Office of the Inspector General (OIG) draft report, Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Benefits Plus (BP) System, 2023-ISAG-007.

Responses to your recommendations including planned corrective actions, as appropriate, are provided below.

Recommendation 1: We recommend that OPM review and update BP's SSP to correct all issues identified during this audit.

Management's Response: Concur. OPM will update BP's SSP to resolve the discrepancies between the security controls matrix (SCM) and the governance, risk, and compliance (GRC) and request AO review and approval of the SSP.

Recommendation 2: We recommend that OPM update BP's SSP to include NIST 800-53, Revision 5, controls that have been selected and implemented to meet the system's security requirements.

Management's Response: Concur. OPM will update BP's SSP to address NIST 800-53, Revision 5.

Recommendation 3: We recommend that OPM complete all scheduled ongoing security control assessments for an entire quarter.

Management's Response: Concur. OPM will complete 3 consecutive months of assessments at the end of June 2023 and will provide documentation to OIG.

Recommendation 4: We recommend that OPM reevaluate the risk response strategy for the untimely POA&Ms identified during this audit, in accordance with organizational risk tolerance.

Management's Response: Concur. OPM is committed to addressing findings in accordance with organizational risk tolerance. We will follow OPM's policy related to risk tolerance and monitoring POA&Ms.

Recommendation 5: We recommend that OPM complete the untimely POA&Ms identified during this audit, in accordance with risk response activities defined by OPM in response to Recommendation 4.

Management's Response: Concur. OPM is committed to addressing findings in accordance with organizational risk tolerance. We will update POA&Ms for BP to comply with OPM's organizational risk tolerance.

Recommendation 6: We recommend that OPM assign a senior official as the AO responsible for authorizing the use of inherited and common controls.

Management's Response: Concur. OPM is finalizing the Assessment & Authorization (A&A) package for the Agency Common Controls (ACC) program. The A&A package will identify the AO.

Recommendation 7: We recommend that OPM ensure that the AO for inherited and common controls that BP has selected to inherit, authorizes BP to inherit those controls

Management's Response: Concur. OPM is finalizing the A&A package for the Agency Common Controls (ACC) program. The AO will authorize the inherited controls.

Recommendation 8: We recommend that OPM identify and document recovery priorities for BP's system components in BP's BIA.

Management's Response: Concur. The BP BIA was updated May 17, 2023 with recovery priorities based on NIST 800-53, Revision 5. OPM notified OIG that the updated version of the BIA is in the A&A package.

Recommendation 9: We recommend that OPM perform a test of BP's contingency plan.

Management's Response: Concur. OPM completed a test of BP's contingency plan on June 1, 2023. OPM will provide the test evidence to OIG under separate cover.

Recommendation 10: We recommend that OPM remediate unsecure configurations identified during this audit using OPM's plan of action and milestones procedures in accordance with an organizational assessment of risk for all affected BP servers and the web application.

Management's Response: Concur. Using OPM's plan of action and milestones procedure, OPM is currently remediating identified unsecure configurations for affected BP servers and web application.

Recommendation 11: We recommend that OPM configure BP's web application to check the validity of internal and external information inputs.

Management's Response: Partially Concur. The text entered in BP is checked by the web application firewall. OPM will review the web application configuration to identify further checks of the validity of information inputs.

Recommendation 12: We recommend that OPM replace or identify extended support for unsupported software identified during this audit for all affected BP servers.

Management's Response: Concur. OPM will remediate unsupported software by upgrading to supported versions of the software.

Recommendation 13: We recommend that OPM install the security-relevant software update identified during this audit for all affected BP servers.

Management's Response: Concur. OPM will install the security-relevant software update identified for affected BP servers.

Recommendation 14: We recommend that OPM review all BP servers for non-compliant configurations identified during this audit and either correct non-compliant configurations or document and approve deviations with a compelling business requirement.

Management's Response: Concur. OPM will review the identified BP servers and will either correct the configuration or document and approve the deviation with the business requirement.

Recommendation 15: We recommend that OPM perform a review of all BP's controls to ensure that all controls have the correct control type and the implementation of each control is described with sufficient detail.

Management's Response: Concur. OPM will review control types and document with sufficient implementation detail to ensure the SSP is compliant with NIST 800-53, Revision 5.

Recommendation 16: We recommend that OPM update BP to generate helpful error messages that are only viewable to defined personnel and do not reveal sensitive information about the system.

Management's Response: Concur. OPM will update and remediate the associated POA&M. We will thereafter provide evidence to OIG to close this recommendation.

We appreciate the opportunity to respond to the draft report. If you have questions, please contact Dennis Hardy (dennis.hardy@opm.gov, 202-606-4182) and David Trzcinski (david.trzcinski@opm.gov, 202-406-0373).

Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in Government concerns everyone: Office of the Inspector General staff, agency employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to OPM programs and operations. You can report allegations to us in several ways:

By Internet: https://oig.opm.gov/contact/hotline

By Phone: Toll Free Number: (877) 499-7295

By Mail: Office of the Inspector General
U.S. Office of Personnel Management
1900 E Street, NW
Room 6400
Washington, DC 20415-1100