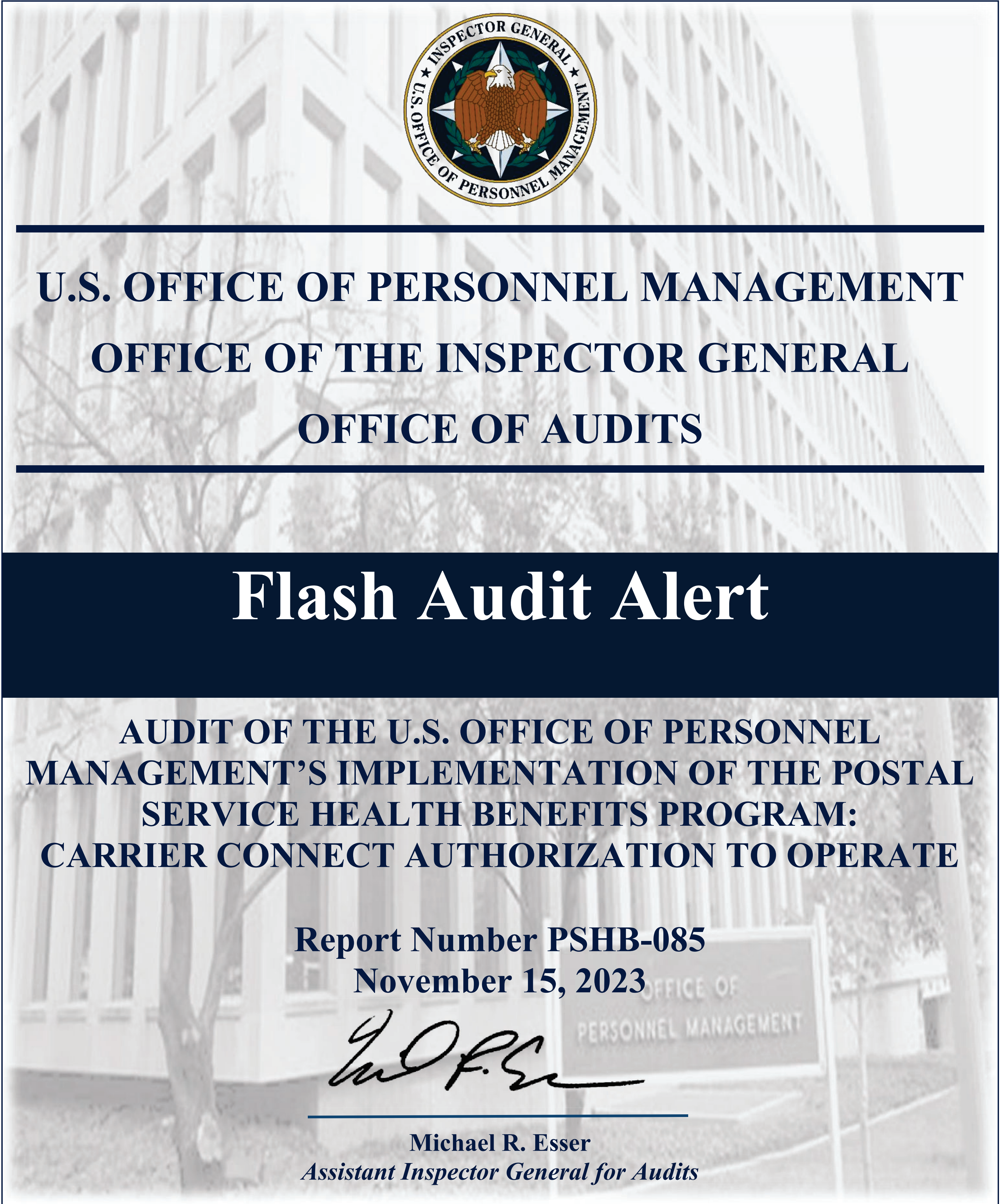

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Flash Audit Alert

AUDIT OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S IMPLEMENTATION OF THE POSTAL SERVICE HEALTH BENEFITS PROGRAM: CARRIER CONNECT AUTHORIZATION TO OPERATE

Report Number PSHB-085
November 15, 2023

Michael R. Esser
Assistant Inspector General for Audits

ABBREVIATIONS

A&A	Assessment and Authorization
AO	Authorizing Official
ATO	Authorization to Operate
FIPS	Federal Information Processing Standards
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPM	U.S. Office of Personnel Management
POA&M	Plan of Action and Milestones
Postal Service	U.S. Postal Service
PSHB	Postal Service Health Benefits
PSHBP	Postal Service Health Benefits Program
PSHBS	Postal Service Health Benefit System
PSRA	Postal Service Reform Act of 2022
SDLC	System Development Life Cycle
SO	System Owner
SP	Special Publication
The Guide	OPM Plan of Action and Milestones Guide

TABLE OF CONTENTS

I. BACKGROUND

The U.S. Office of Personnel Management (OPM) Office of the Inspector General (OIG) is responsible for performing oversight of OPM's implementation of the Postal Service Health Benefits Program (PSHBP).

The PSHBP was established within the Federal Employees Health Benefits Program (FEHBP) by Public Law 117-108, the Postal Service Reform Act of 2022 (PSRA), enacted on April 6, 2022. The PSHBP will be administered by OPM's Healthcare and Insurance Office. The PSHBP was created to provide health insurance benefits for U.S. Postal Service (Postal Service) employees, annuitants, and dependents beginning on January 1, 2025. For these individuals, eligibility for enrollment or coverage in Federal Employees Health Benefits plans will end on December 31, 2024, and enrollment and coverage will only be offered by Postal Service Health Benefit (PSHB) plans after that time. Subject to limited exceptions, Postal Service annuitants who retire and become Medicare-eligible after December 31, 2024, and their Medicare-eligible[1] family members, will be required to enroll in Medicare Part B[2] as a condition of eligibility to enroll in the PSHBP. The first Open Season for the PSHBP will begin on November 11, 2024, and run through December 9, 2024. The first contract year will begin January 1, 2025.

Section 101 of the PSRA added a new section, 8903c, to 5 U.S.C. Chapter 89 which directs OPM to establish the PSHBP. The PSHBP was authorized under the Title I Postal Service Financial Reforms provisions in the PSRA in furtherance of Congress's objective to "improve the financial position of the Postal Service while increasing transparency and accountability of the Postal Service's operations, finances, and performance." OPM issued an interim final rule on April 6, 2023, to set forth standards to implement Section 101 of the PSRA to establish the PSHBP.

OPM is developing an electronic centralized enrollment process simultaneously with the implementation of the PSHBP. The centralized enrollment process will be an electronic enrollment solution for all PSHB stakeholder groups including enrollees, the Postal Service, other employing offices, and PSHB Carriers. The electronic enrollment process is comprised of two systems, Carrier Connect and the Postal Service Health Benefit System (PSHBS). The Carrier Connect system serves as a record between OPM and health insurance carriers for proposals, contracting decisions, communication, and data. The PSHBS will include an online portal to enter and process enrollment transactions, robust decision support tools, as well as a customer support center to assist enrollees through phone, email, or online chat.

The intent of this flash audit alert is: (1) to ensure OPM addresses the audit findings described on pages 3 through 9 in a timely manner; and (2) to ensure that OPM completes critical security documentation in accordance with relevant policies, procedures, and guidance during the future

[1] Medicare is generally for people 65 or older, but may also include people with disabilities, End-Stage Renal Disease, or Lou Gehrig's disease.

[2] Medicare Part B is medical insurance covering services from doctors, outpatient care, home health care, durable medical equipment, and many preventative services.

development of PSHB information technology (IT) systems. The findings in this report are specific to the Carrier Connect's assessment and authorization (A&A) process and the associated security documentation that was not completed during the system development life cycle (SDLC).

II. AUDIT FINDINGS AND RECOMMENDATIONS

ASSESSMENT AND AUTHORIZATION

The primary challenge facing OPM in the implementation of the PSHBP is the requirement that postal employees be enrolled in a PSHB plan by January 1, 2025. This means that the IT systems supporting the enrollment process must be securely developed, tested, and operational well before the FY 2025 open season enrollment period that starts in November 2024. The Carrier Connect system had an even shorter development timeline because the system was scheduled to be moved into the OPM production IT environment by the end of June 2023 to support the application process for health insurance carriers to participate in the new PSHBP.

An important aspect of the SDLC is the foundational concept that information security be considered and incorporated throughout the process. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Rev. 2 "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy" discusses this in detail.

NIST 800-37 states:

> Security and privacy requirements are part of the functional and nonfunctional requirements allocated to a system. The security and privacy requirements are incorporated into the SDLC simultaneously with other requirements. Without the early integration of security and privacy requirements, significant expense may be incurred by the organization later in the life cycle to address security and privacy concerns that could have been included in the initial design. When security and privacy requirements are defined early in the SDLC and integrated with other system requirements, the resulting system has fewer deficiencies, and therefore, fewer privacy risks or security vulnerabilities that can be exploited in the future.

Similarly, the DevSecOps (short for development, security, and operations) approach to systems development and Microsoft's Security Development Lifecycle emphasize the integration of security at every phase of the lifecycle from initial design through testing and delivery.

We found, however, that because of the strict deadline, OPM did not effectively plan and execute the security assessment and authorization phase of the Carrier Connect SDLC. IT security was not integrated at the beginning and as a result many of the required elements of an authorization to operate (ATO) package were not completed before the system was authorized to operate and placed into production. For example, the system security categorization (Federal Information Processing Standards (FIPS) 199) and the system security plan were not completed before the authorization memo was signed by the authorizing official.

The FIPS 199 system security categorization process describes the security level of the system based on a common framework and is the first step in developing appropriate IT security for a system. The purpose of a system security plan is to document the structured process of planning effective security protection. It defines the system boundaries and the applicable security controls based on the FIPS 199 categorization. These fundamental planning documents were not completed until nearly three months after the system was authorized to operate and placed into production.

We also found that OPM did not adequately manage the plan of action and milestones (POA&M) process as part of this security assessment. Almost all of the POA&Ms associated with control weaknesses identified during the assessment were still not finalized more than three months after they were first documented. This step is required before corrective action can begin. Finally, the authorization itself was considered, according to OPM's Authorization Memorandum, a provisional document with embedded conditions and a shortened timeframe, indicating that OPM officials were aware that the security assessment was inadequate to support a full ATO. Provisional ATOs are not consistent with the NIST Risk Management Framework unless a system is being placed into a production environment for the sole purpose of limited testing, which was clearly not the case for Carrier Connect because the system was in production for carriers to submit applications for participation in the PSHBP.

As a result of OPM's flawed security assessment and authorization process, it is possible that unknown security vulnerabilities in the Carrier Connect system have increased the risk of a significant security incident. This could potentially impact the agency's ability to successfully implement the requirements of the PSRA. There is also the potential for greater risk that attackers could establish a foothold in OPM's IT environment and compromise enterprise-wide security.

Because of the urgent and time sensitive nature of the material presented in this flash audit alert, we did not issue a draft report to obtain the views of responsible management officials. We did, however, discuss our findings with OPM management officials on September 25, 2023. We subsequently met with senior officials from OPM's Office of the Chief Information Officer (OCIO) on September 28, 2023, to clarify some of the issues associated with this authorization process.

OPM OCIO officials acknowledged that the A&A process started too late in the SDLC, in the summer of 2023, and that they knew the authorization decision would have to be provisional. Specifically, the Carrier Connect Authorization Memorandum[3] stated, "Considering the

[3] Memorandum signed on June 26, 2023, by the authorizing official for the Authorization to Operate – Carrier Connect.

overarching mission requirement for [Carrier Connect] to operate, I am issuing a provisional [Authorization to Operate] ATO not to exceed December 26, 2023."

OCIO officials stated that because of long-standing problems with system security plans, they wanted to ensure the quality of the process and the supporting documents, which took longer. We were also told that since the initial version of Carrier Connect is considered a minimally viable product and there is no personally identifiable information in the system, it was viewed to be lower risk.

In addition, OCIO officials commented that functional testing of a system's security can provide better insight than point-in-time documents. For example, OPM conducted a penetration test of Carrier Connect to better understand system vulnerabilities, and the agency's IT security team routinely leverages all available security tools to continuously monitor all systems.

OCIO officials believe that the question of a provisional ATO is a "nomenclature issue" rather than a cause for concern. They stated that this was not an "interim" ATO but that it had limits to ensure that the processes are completed.

OPM's Chief Information Officer noted that in the past, there were several OPM systems operating without a proper ATO, that he views the issue very seriously, and that his team is working hard to ensure that all systems have a proper ATO. He also stated that there were lessons learned from the Carrier Connect security A&A process. For the PSHBS development, there will be more staff assigned and the security assessment will start earlier in the SDLC.

OPM has made great strides in recent years improving its overall IT security program, as documented in our recent Federal Information Security Modernization Act audit reports. The agency has improved technical security controls and is focusing on its zero-trust networking strategy. However, functional and technical security controls, such as those relied upon by the OCIO in this case, complement rather than replace proper IT security planning and documentation.

We appreciate that OPM's OCIO understands the risks involved with the Carrier Connect ATO and is working to implement improved processes for the upcoming development of the PSHBS. It will be even more important for OPM to not only develop the functional requirements of this system, but also to ensure that it is properly secured. Carrier Connect is an important system that serves as a key part of program planning, but PSHBS will be the actual centralized enrollment portal that will directly affect the success of the entire project. It is critical that established SDLC principles are strictly enforced.

A security authorization package should contain all security documents required for the Authorizing Official (AO) to make an ATO decision. We reviewed the Carrier Connect security authorization package to determine if the required documents were completed in accordance with

OPM policy, Office of Management and Budget (OMB) guidance, and the NIST Risk Management Framework.

The Carrier Connect ATO documents reviewed by the OIG included:

- The FIPS 199 Security Categorization document;
- The Privacy Threshold Analysis and Privacy Impact Assessment;
- The System Security Plan;
- Security and Risk Assessments;
- Information Security Continuous Monitoring;
- POA&Ms; and
- The Authorization Memorandum.

The following discussion highlights the detailed findings and recommendations associated with our review of the Carrier Connect security assessment and authorization.

1. FIPS 199 Security Categorization

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 the Federal information or information system was assigned using FIPS Publication 199 guidance.

OPM had not finalized Carrier Connect's *FIPS 199 Security Categorization* document prior to the ATO decision. The system's *Security Assessment Plan* identifies the *FIPS 199 Security Categorization* as one of the documents needed to begin a security controls assessment.

The *OPM Security Authorization Guide* states that "The baseline set of controls is selected based on the FIPS 199 categorization and is then tailored to meet the specific security and privacy requirements of the system."

NIST SP 800-37, Revision 2, states that during the initiation phase of the SDLC for new systems, impact levels are determined for each information type and for each security objective (i.e., confidentiality, integrity, and availability) and that security categorization is based on a high-water mark of information type impact levels.

Failure to finalize Carrier Connect's security categorization during the A&A process prior to a security controls assessment, increases the risk that security controls were not appropriately implemented and tested.

2. System Security Plan

OMB Circular A-130, *Managing Information as a Strategic Resource*, requires a system security plan to be developed for all Federal information systems. The system security plan provides an overview of the system security requirements and describes the controls that are in place or planned to meet those requirements.

OPM had not finalized Carrier Connect's system security plan prior to the ATO decision. The system's *Security Assessment Plan* identifies the system security plan as one of the documents needed to define system boundaries and descriptions of security controls for the approved control selection and is needed to develop the *Security Assessment Plan*.

OPM's *Security Planning Policy* states that the system security plan is reviewed and approved by the AO prior to implementation.

NIST SP 800-37, Revision 2, states that during the initiation phase of the SDLC for new systems, "security categorization information is documented in the system security plan … ."

For Federal information systems to be granted an 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 system security plan establishes and documents security controls for the system and is the basis for the authorization. Failure to finalize the system security plan, prior to an ATO decision, increases the risk that the AO may not have had the necessary information to make an informed risk-based decision.

3. Plan 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.

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

We reviewed Carrier Connect's POA&Ms and identified that 54 out of 55 total POA&Ms were in a "draft" status as of September 19, 2023. All POA&M items were assigned a risk categorization of Moderate or High and were added to OPM's centralized tracking dashboard on June 15, 2023. The *OPM Plan of Action and Milestones Guide* (The Guide) states that the target timeframe for remediating High risk items is 30 days and the target timeframe for remediating Moderate risk items is 60 days. The Guide also states that POA&Ms in a "draft" status have identified milestones, resources, and evidence to demonstrate closure. However, the evidence to demonstrate closure needs to be reviewed and approved by the Management Review Board before the POA&M can be moved to an "open" status. As of September 19, 2023, over three months after the POA&M items were documented for tracking purposes, none of the risks identified in the POA&Ms had been remediated. According to the authorization memorandum, one of the tasks that needs to be completed by the System Owner (SO), as a contingency for the ATO, is to mitigate and/or remediate any "open" POA&Ms.

NIST SP 800-37, Revision 2, states that during the implementation phase of the SDLC for new systems, POA&Ms are included as part of the authorization package. Furthermore, NIST SP 800-37, Revision 2, states that POA&Ms are informed by the security categorization of the system and security and privacy . . . risk assessments."

Failure to update the status of "draft" POA&Ms, in accordance with OPM policy, increases the risk that system weaknesses will not be remediated in a timely manner.

4. Carrier Connect Authorization Memorandum

OMB Circular A-130, *Managing Information as a Strategic Resource*, requires all Federal information systems to have a valid authorization. An authorization memorandum is an official management decision to authorize a system to operate and accept its known risks.

The Carrier Connect authorization memorandum was signed by the AO on June 26, 2023, provisionally authorizing the system to operate for a period of six months. The ATO was contingent upon the SO completing several tasks, which included finalizing security documentation according to OPM policy. As discussed above, critical security documentation required by the AO to make an informed risk-based decision was not completed prior to the ATO.

The *OPM Security Authorization Guide* states that the AO is responsible for approving the

A&A package as part of the formal authorization process. OMB Circular A-130, *Managing Information as a Strategic Resource*, states that "At a minimum, the authorization package includes the information system security plan, privacy plan, security control assessment, privacy control assessment, and any relevant plans of action and milestones."

NIST SP 800-37, Revision 2, states that during the implementation phase of the SDLC for new systems, "the authorization package is used by authorizing officials to make informed, risk-based decisions."

Failure to finalize all necessary A&A documentation prior to an ATO decision increases the risk that the AO may not have had the necessary information to make an informed risk-based decision.

RECOMMENDATIONS

The following recommendations are being issued to address the findings discussed above.

Recommendation 1

We recommend that OPM finalize the incomplete Carrier Connect authorization security documentation (i.e., FIPS 199, system security plan, and POA&Ms) prior to the expiration of the six-month provisional ATO.

Recommendation 2

We recommend that OPM ensure that security considerations are properly integrated with all phases of the system development lifecycle for the PSHBS and any other new PSHB IT systems, and that proper security assessment and authorization processes and documentation are completed prior to the authorization decision.

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