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 Executive Schedule C System

Report Number 4A-ES-00-21-020
September 30, 2021

Executive Summary

Audit of the Information Security Controls of the U.S Office of Personnel Management's Executive Schedule C System

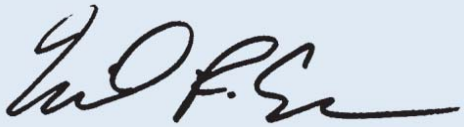
Report No. 4A-ES-00-21-020 **September 30, 2021**

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 including testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems. The Executive Schedule C System (ESCS) has been included in this year's representative subset of systems because it is one of the Office of Personnel Management's (OPM) major systems.

What Did We Audit?

The Office of the Inspector General completed a performance audit of ESCS's information technology (IT) security controls to ensure that it meets the standards established by FISMA, the National Institute of Standards and Technology, and OPM's Office of the Chief Information Officer.



Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit of ESCS's IT security controls determined that:

- The ESCS Privacy Impact Assessment incorrectly describes the system's operational environment.
- The ESCS Security Controls Matrix includes some control descriptions that are inaccurate or incomplete.
- A Plan of Action and Milestones (POA&M) has not been created for all weaknesses identified.
- POA&Ms were closed after the scheduled completion date or remained open after the scheduled completion date.
- OPM did not provide security configuration standards or baseline configurations for ESCS servers.
- Vulnerability scans of ESCS servers are not authenticated with privileged credentials.
- Vulnerability scans of the ESCS web application identified a "High" severity vulnerability.
- ESCS does not have adequate event auditing controls.
- The ESCS System Security Plan, Contingency Plan, and Business Impact Analysis include conflicting system inventories.
- Controls are not in place to track ESCS software license usage.
- Controls are not in place to disable access to the ESCS web application in a timely manner upon employment termination.
- Unit integration testing is not performed for ESCS web application code modifications.

Abbreviations

DISA	**Defense Information Systems Agency**
ESCS	**Executive Schedule C System**
FIPS	**Federal Information Processing Standards**
FISMA	**Federal Information Security Modernization Act**
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**
POA&M	**Plan of Action and Milestones**
PTA	**Privacy Threshold Analysis**
SAP	**Security Assessment Plan**
SCM	**Security Controls Matrix**
SP	**Special Publication**
SSP	**System Security Plan**
STIG	**Security Technical Implementation Guide**

Table of Contents

Report Fraud, Waste, and Mismangement

I. Background

On December 17, 2002, the President signed the E-Government Act (P.L. 107-347) into law, which includes Title III, the Federal Information Security Management Act (FISMA). It requires (1) annual agency program reviews, (2) annual Inspector General evaluations, (3) agency reporting of the results of Inspector General 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, Public Law 113-283, FISMA, was established and reaffirmed the objectives of the prior FISMA. Public Law 113-283 states that each year, the Office of the Inspector General (OIG) shall perform an independent evaluation of the Office of Personnel's (OPM) information security program and practices to determine its effectiveness. This includes the testing of a representative subset of the agency's information systems.

The Executive Schedule C System (ESCS) has been included in this year's subset of systems because it is one of OPM's moderate risk, major systems, and an audit of its information technology (IT) security controls has not been conducted within the past 10 years. According to the ESCS System Security Plan (SSP), "ESCS is a human resources application that is used to collect and maintain information on career and non-career Senior Executive Service (SES) personnel, other executive personnel, and non-career non-executive employees on Schedule C appointments."

The OPM Office of the Chief Information Officer (OCIO) has responsibility for implementing and managing the IT security controls of ESCS. We discussed the results of our audit with OPM representatives during the exit conference for this audit.

II. Objective, Scope, and Methodology

Objective

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

Scope and Methodology

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards, issued by the Comptroller General of the United States. Accordingly, the audit included an evaluation of related policies and procedures, compliance tests, and other auditing procedures we considered necessary. The audit covered FISMA compliance efforts of OPM officials responsible for the ESCS and security controls in place as of July 2021.

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

- Federal Information Processing Standards publication 199 (FIPS 199) Analysis;
- Privacy Impact Assessment (PIA);
- System Security Plan;
- Security Controls Assessment;
- Continuous Monitoring;
- Plan of Action and Milestones (POA&M);
- Authorization Memo;
- Contingency Planning; and
- NIST Special Publication (SP) 800-53, Revision 4, Security Controls.

We considered the ESCS 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.

As appropriate, we conducted compliance tests to determine the extent to which established controls and procedures are functioning as required. We evaluated whether a sample of 48 NIST SP 800-53 controls were implemented for the ESCS. Controls were selected that related to the system's Authorization package, vulnerability scanning, and patching. Additionally, we reviewed controls that were not tested during the most recent independent security assessment or had identified weaknesses with no corresponding POA&M. Test methods included interviews of

OPM representatives with IT security responsibilities related to the ESCS, review of system screenshots and output, observation of system capabilities, and vulnerability scanning. All systems within the ESCS's system boundary were included in our controls testing. The results of tested controls selected using judgmental sampling cannot be projected to the entire universe of NIST SP 800-53 controls population since it is unlikely that the results are representative of the entire population of controls.

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.

The criteria used in conducting this audit include:

- E-Government Act of 2002 (P.L. 107-347), Title III, Federal Information Security Management Act of 2002;
- Public Law 113-283, Federal Information Security Modernization Act of 2014;
- 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 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations;
- NIST SP 800-60, Revision 1, Volume II, Guide for Mapping Types of Information and Information Systems to Security Categories;
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems;
- OMB's Circular A-130, Appendix I;
- OPM Security Planning Policy;
- OPM Security Authorization Guide;
- OPM Risk Management Policy;
- OPM Information Technology Security FISMA Procedures; and
- OPM Archer User Guide.

Details of the security controls protecting the confidentiality, integrity, and availability of the ESCS are in section III of this report, "Audit Findings and Recommendations." Since our audit would not necessarily disclose all significant matters in the internal control structure, we do not express an opinion on the ESCS internal controls taken as a whole.

The OPM Office of the Inspector General, as established by the Inspector General Act of 1978, as amended, performed the audit. We conducted the audit remotely from February 2021 through July 2021 in the Washington, D.C. area.

Compliance With Laws and Regulations

In conducting the audit, we performed tests to determine whether OPM's management of the ESCS is consistent with applicable standards. While generally compliant, with respect to the items tested OPM was not in complete compliance with all standards, as described in section III of this report, "Audit Findings and Recommendations."

III. Audit Findings and Recommendations

A. FIPS 199 Analysis

Security categorization controls are adequate.

The E-Government Act of 2002 requires Federal agencies to assign a security categorization to all Federal information and information systems. FIPS Publication 199 defined standards to be used by federal agencies to categorize information systems based on appropriate levels of information security according to risk. Minimum information security requirements of each information system are determined based on the system's security categorization assigned using FIPS Publication 199 guidance.

NIST SP 800-60, Revision 1, Volume II, provides an overview of the security objectives and impact levels identified in FIPS 199.

The security categorization document includes an analysis of the information processed by the ESCS and the corresponding impact of confidentiality, integrity, and availability. The ESCS is categorized as a "moderate" impact level for each area – confidentiality, integrity, and availability – resulting in an overall categorization of "moderate."

The security categorization of the ESCS appears to be consistent with FIPS 199 and NIST SP 800-60, Revision 1, Volume II requirements, and we agree with the categorization of "moderate." Additionally, the requirements of NIST SP 800-53, Revision 4, control RA-2 Security Categorization, have been adequately implemented.

No opportunities for improvement related to the ESCS FIPS 199 security categorization were identified.

B. Privacy Impact Assessment

The E-Government Act of 2002 requires agencies to conduct 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.

A PTA was performed for the ESCS in July 2020 and concluded that a PIA was required. The PTA included a privacy controls assessment which had not been updated since 2018. The opportunity for improvement was brought to OPM's attention and the privacy controls assessment was immediately updated with current assessment results.

The ESCS PIA was completed and formally approved by the Chief Privacy Officer in October 2020. However, we identified the following opportunities for improvement during our review of the ESCS PIA.

1. Operational Environment Documentation

The PIA does not accurately depict risk.

The ESCS PIA contains incorrect statements about the system's current operational environment. Specifically, that to mitigate the risk of inaccurate data entry, the ESCS uses structured query language to automatically retrieve data from the Enterprise Human Resources Integration Data Warehouse system. The PIA, which was created in October 2020, reflects an operational environment that is planned but has not yet been implemented. During this audit, OPM updated the PIA to reflect the current operational environment. However, it is still awaiting approval, and the public version of the PIA remains inaccurate.

NIST SP 800-53, Revision 4, control AR-2 (b.) Privacy Impact and Risk Assessment, states that the organization "Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures."

Without a correct depiction of the ESCS's operational environment, an accurate PIA cannot be produced.

Recommendation 1

We recommend that OPM update the ESCS's public PIA to reflect the system's current operational environment.

OPM's Response:

"Based on the notice of Findings and Recommendations, shared with us by the CIO and Employee Services, we updated the ESCS PIA to reflect the current environment. The Chief Privacy Officer approved and signed the revised PIA, effective July 22, 2021 (see attached document) and in accordance with OPM practice, the final PIA was sent to the Director's office for instruction to the Office of Communications to post to the OPM public site. The PIA is now available for public viewing. As this issue was remediated, we ask that the recommendation be removed from the final report."

OIG Comment:

In response to the draft audit report, OPM has updated its public facing PIA for the ESCS. The PIA now accurately reflects the system's current operational environment. The intent of this recommendation has been addressed. No further action is required.

C. System Security Plan

Federal agencies must implement the security controls outlined in NIST SP 800-53, Revision 4, for each information system. NIST SP 800-18, Revision 1, requires that these controls be documented in an SSP for each system and provides guidance for doing so. The Security Controls Matrix (SCM) is a document OPM uses to supplement each system's SSP. It includes descriptions of how each applicable control is implemented and a rationale for not implementing controls determined not to be applicable.

The ESCS SSP satisfies some of the control requirements in NIST SP 800-53, Revision 4, control PL-2 System Security Plan, including, but not limited to:

- Explicitly defining the authorization boundary for the system;
- Describing the operational context of the system in terms of mission and business processes; and
- Providing an overview of the security requirements for the system.

However, we identified the following opportunities for improvement during our review of the ESCS SSP.

1. Security Controls Matrix

The OIG reviewed the ESCS SCM and determined the following:

- The ESCS's description of some controls suggests that the control type is inaccurate;
- The ESCS's description of some controls does not address all the control requirements;
- The ESCS's description of some controls does not effectively address the control requirements; and
- The ESCS's description of some controls does not accurately describe the system.

The ESCS has not performed an analysis of each control to determine how or if the system satisfies each control requirement.

NIST SP 800-53, Revision 4, control PL-2 (a. 8. and c.) System Security Plan, states that the organization "Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions …" and "Reviews the security plan for the information system [the organization-defined frequency] … ." OPM's Security Planning Policy defines this frequency as annually.

Failure to accurately document the ESCS's controls negatively impacts OPM's ability to understand the system's security posture.

Recommendation 2

We recommend that OPM routinely review and update the ESCS SCM to ensure that controls are accurately documented and effectively satisfy all control requirements.

OPM's Response:

"We concur. The system ISSO, program office and process owners meet bi-weekly to review and update the ESCS security control matrix. The purpose of the bi-weekly meeting is to ensure that all controls are accurately documented in the SCM to a level that fully satisfies control requirements. The bi-weekly meetings will continue until all applicable ESCS security controls have been reviewed and verified with artifacts. The meeting agenda and post-meeting recap document the remediation efforts discussed during the meeting. OPM will provide supporting artifacts with the completed SCM."

OIG Comment:

As part of the audit resolution process, please 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 the OCIO agrees to implement.

D. Security Controls Assessment

Security assessment controls are adequate.

A Security Assessment Plan (SAP) describes the scope, procedures, environment, team, roles, and responsibilities for an assessment to determine the effectiveness of a system's security controls. The Security Assessment Report presents the results of the SAP and includes a review of management, operational and technical security controls. The Risk Assessment Table maintains the list of a system's security controls with identified weaknesses, including the likelihood of harm and the potential threat impact to the agency.

OPM tests all of a system's applicable controls over a three-year period. An independent security controls assessment of a subset of controls is performed tri-annually. The remaining controls are tested during the system's continuous monitoring activities. We reviewed the ESCS's most recent SAP for an independent security controls assessment, performed July through August 2019. The results of the tests performed were documented and shared with the system's Authorizing Official in a Quality Assurance memo. We also reviewed continuous monitoring reports completed within the tri-annual period and verified that an acceptable portion of the system's applicable controls were tested. We determined the security assessment was

appropriate and requirements of NIST SP 800-53, Revision 4, control CA-2 Security Assessments, have been adequately implemented.

No opportunities for improvement related to the ESCS security controls assessment were identified.

E. Continuous Monitoring

Continuous monitoring controls are adequate.

OPM requires that the IT security controls of each system be assessed on a continuous basis. OPM's OCIO has developed an Information Security Continuous Monitoring Plan that includes a template outlining the security controls that must be tested for all information systems. All system owners are required to tailor the Information Security Continuous Monitoring Plan template to each individual system's specific security control needs and then test the system's security controls on an ongoing basis. The test results must be provided to the OCIO on a routine basis for centralized tracking.

We reviewed the ESCS's quarterly continuous monitoring submissions for fiscal year (FY) 2020 and quarter one of FY 2021, and concluded that requirements of NIST SP 800-53, Revision 4, control CA-7 Continuous Monitoring, have been adequately implemented.

No opportunities for improvement related to the ESCS's continuous monitoring strategy were identified.

F. Plan of Action and Milestones

A POA&M is a form of action plan used by agencies to identify, assess, prioritize, and monitor the progress of corrective efforts for known IT security weaknesses. OPM has implemented an agency wide POA&M process to help track known IT security weaknesses associated with the agency's information systems.

The OIG reviewed all ESCS POA&Ms from FY 2020 and quarter one of FY 2021. The following opportunities for improvement were identified.

1. Missing POA&Ms

Twenty-three identified weaknesses do not have POA&Ms.

POA&Ms have not been created for all weaknesses identified in the ESCS's various assessments of security controls, including:

- 12 out of the 19 controls listed as "Planned" in the ESCS SCM;

- 4 out of the 32 weaknesses identified during the ESCS's last security controls assessment; and

- 7 out of the 25 weaknesses identified in the ESCS's FY 2020 Continuous Monitoring Report.

OPM is not cross referencing the ESCS's assessment results with the list of current POA&Ms to ensure that each identified weakness has a POA&M.

NIST SP 800-53, Revision 4, control CA-5 (a.) Plan of Action and Milestones, states that the organization "Develops a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies … ." Additionally, the OPM Security Authorization Guide states that "All risks that have not been remediated must be documented in the POA&M including risks from controls inherited from other systems, risks from the independent assessment, and any pre-defined risks."

Failure to develop a POA&M for identified weaknesses increases the probability that weaknesses will not be mitigated within a reasonable timeframe.

Recommendation 3

We recommend that OPM create a POA&M for all controls listed as "Planned" in the SCM, weaknesses identified during the last security controls assessment, and weaknesses identified during FY 2020 continuous monitoring.

OPM's Response:

"We concur. OPM requests that this recommendation be removed from the final audit report. OPM has documented the POA&Ms for all controls identified as planned in the SCM and the weaknesses previously identified in FY2020 continuous monitoring. The POA&Ms identified during the last security assessment have been reviewed to determine if they are applicable. These POA&Ms will be tracked and maintained as milestones are completed and updates are provided. Evidence of these POA&Ms are included with this report response."

OIG Comment:

In response to the draft audit report, OPM provided evidence that POA&Ms have been created for some of the weaknesses that were previously missing POA&Ms. However, the intent of this recommendation is for OPM to create POA&Ms for all identified weaknesses. As part of the audit resolution process, please provide OPM's Internal Oversight and Compliance office with evidence that this recommendation has been implemented.

2. POA&M Timeliness

We identified that 34 out of the 47 POA&Ms were either closed after the scheduled completion date or remained open after the scheduled completion date. The Information System Security Officer is not updating the scheduled completion date to reflect current timelines based on reviews of remediation activities.

Thirty-four of 47 POA&Ms were not completed on time.

NIST SP 800-53, Revision 4, control CA-5 (b) Plan of Action and Milestones, states that the organization "Updates existing plan of action and milestones [the organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities." OPM's Risk Management Policy defines this frequency as weekly. OPM 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." The OPM Archer User Guide defines the "Scheduled Completion Date" field as a reasonable timetable for completion.

Failure to routinely reassess scheduled completion dates increases the risk that mitigating controls will not be implemented within a reasonable timeframe.

Recommendation 4

We recommend that OPM perform and document a reassessment of the scheduled completion date for all open ESCS POA&Ms that have surpassed the scheduled completion date.

OPM's Response:

"We concur. The scheduled completion date that is initially provided during the evaluation and documentation of the POA&M signifies the date that Employee Services aims to resolve the vulnerability. Due to unexpected circumstances, such as unsuccessful remediations, limited resources, or additional time required to complete the tasks identified in the milestones, the scheduled completion date is often reevaluated. The revised date is tracked as the Expected Completion Date. OPM will review the original and revised dates to ensure that they are on or after the submission date."

G. Authorization Memo

The Authorization Memo is an official management decision to authorize operation of an information system and accept known risks. OMB's Circular A-130, Appendix I, mandates that all Federal information systems have a valid

Security authorization controls are adequate.

Authorization. Although OMB previously required periodic Authorizations every three years, Federal agencies now have the option of continuously monitoring their systems to fulfill the Authorization requirement. OPM does not yet have a mature program in place to continuously monitor system security controls; therefore, a current Authorization is required for all OPM systems at least once every three years as required by OPM policy.

The ESCS was authorized to operate in April 2021. The Authorization is valid until October 2022 and is contingent on the remediation of several ESCS IT security weaknesses included in the document. During this audit, we observed that many of these weaknesses have been remediated. The ESCS Authorization Memo meets the requirements of NIST SP 800-53, Revision 4, control CA-6 Security Authorization.

No opportunities for improvement related to the ESCS Authorization were identified.

H. Contingency Planning

Contingency planning controls are adequate.

NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems, states that effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability. OPM's security policies require all major applications to have viable and logical disaster recovery and contingency plans, and that these plans be annually reviewed, tested, and updated.

The ESCS contingency plan meets the requirements of NIST SP 800-53, Revision 4, control CP-2 Contingency Plan and CP-2 (3.) Contingency Plan | Resume Essential Missions / Business Functions.

OPM did not provide evidence of the implementation of NIST SP 800-53, Revision 4, control CP-4 Contingency Plan Testing, which requires the contingency plan to be tested annually. The documentation provided suggests that the last contingency plan test was performed in 2012. However, OPM is aware of the weakness and is appropriately tracking its remediation using a documented POA&M.

No opportunities for improvement related to the ESCS's contingency planning were identified.

I. Vulnerability Scanning

As part of this audit, OPM conducted vulnerability and compliance scans of all of the ESCS servers and vulnerability scans of the ESCS web application, on our behalf. Additionally, we reviewed a sample of OPM's historical scans of the ESCS servers and the web application.

The results of our vulnerability scanning exercise demonstrate that OPM has adequately implemented the following NIST SP 800-53, Revision 4, controls:

- RA-5 Vulnerability Scanning;
- SA-22 Unsupported System Components;
- SI-2 Flaw Remediation; and
- SI-2 (2) Flaw Remediation | Automated Flaw Remediation.

However, we identified the following opportunities for improvement related to OPM's vulnerability and configuration management program.

1. Configuration Settings

OPM has not documented configuration settings for technology products employed within the ESCS system boundary that reflect the most restrictive mode consistent with operational requirements. OPM uses Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) compliance files to monitor the configuration of the ESCS servers. However, the implementation of every DISA STIG configuration is not consistent with operational requirements. OPM has not documented the tailored version of the DISA STIG standards that are appropriate for its system. Therefore, we were unable to complete our analysis of compliance scan results to determine whether the ESCS systems are configured appropriately.

NIST SP 800-53, Revision 4, control CM-6 (a.) Configuration Settings, requires that the organization "Establishes and documents configuration settings for information technology products employed within the information system … that reflect the most restrictive mode consistent with operational requirements … ."

Without documented configuration settings, OPM has no reference to verify whether settings are configured in accordance with approved security standards and least functionality principles.

Recommendation 5

We recommend that OPM establish and document configuration settings for technology products employed within the ESCS system boundary that reflect the most restrictive mode consistent with operational requirements.

OPM's Response:

"We concur. OPM will review the technology products contained within the ESCS system boundary, ensuring that this boundary is clearly defined and that all relevant inherited controls are considered. Once the technology products have been verified, we will

establish and document the system specific configuration settings. Our target completion date for this recommendation is Fiscal Year 2022 Q3."

2. Privileged Vulnerability Scanning

Vulnerability scans of the ESCS servers identified unsupported software that OPM has since removed. OPM stated that the reason unsupported software was not identified in prior scans was because privileged credentials are not used to authenticate vulnerability scans of the ESCS servers. Following our advisory that vulnerability scans should be authenticated using privileged credentials, OPM attested that this control has been implemented. However, we have not received sufficient evidence to support this claim.

NIST SP 800-53, Revision 4, control RA-5 (5) Vulnerability Scanning | Privileged Access, states that "The information system implements privileged access authorization to [the organization identified information system components] for selected [organization-defined vulnerability scanning activities]."

Without privileged credentials, vulnerability scanning tools will not have the required level of system access to identify all vulnerabilities.

Recommendation 6

We recommend that OPM use privileged credentials to authenticate vulnerability scans of the ESCS servers.

OPM's Response:

"We concur. OPM requests that this recommendation is removed from the final audit report. This finding was remediated on June 24, 2021. OPM has configured vulnerability scanning tools to execute privileged scans on ESCS as was previously configured. Documentation to show the updated scanning credentials is enclosed."

OIG Comment:

In response to the draft audit report, OPM provided screenshots demonstrating that vulnerability scans are authenticated with credentials. However, the intent of this recommendation is to ensure vulnerability scans are authenticated with privileged credentials. Based on the evidence provided, we are unable to determine if these credentials have privileged access.

3. Web Application Vulnerability

During a review of historical ESCS web application vulnerability scans, we observed that a "High" severity vulnerability was identified. The ESCS web application uses a weak random number generator to create session tokens.

NIST SP 800-53, Revision 4, control RA-5 (d.) Vulnerability Scanning, states that the organization "Remediates legitimate vulnerabilities [the organization-defined response times] in accordance with an organizational assessment of risk … ."

Failure to remediate vulnerabilities increases the risk that hackers could exploit system weaknesses for malicious purposes.

Recommendation 7

We recommend that OPM remediate the specific technical weakness discovered during this audit.

OPM's Response:

"We concur. A POA&M for the weakness has been documented and is being tracked. This POA&M has been discussed in the ESCS bi-weekly POA&M review meeting. An action plan is being set forth for remediation and is expected to be completed in FY22 Q1."

J. NIST SP 800-53 Controls Testing

ESCS satisfied 19 of the 48 controls tested.

NIST SP 800-53, Revision 4, 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. As part of this audit, we evaluated whether OPM has implemented a subset of these controls for the ESCS. We selected controls related to the system's Authorization package, vulnerability scanning, and patching. Additionally, we reviewed controls that were not tested during the most recent independent security assessment or had identified weaknesses with no corresponding POAM. A total of 48 controls were tested including one or more controls from each of the following control families:

- Access Control;
- Accountability, Audit, And Risk Management;
- Audit and Accountability;
- Configuration Management;
- Contingency Planning;
- Identity and Authentication;
- Personnel Security;
- Planning;

- Risk Assessment;
- Security Assessment and Authorization;
- System and Communications Protection;
- System and Information Integrity; and
- System and Services Acquisition.

OPM demonstrated that 19 of the tested controls have been adequately implemented. Weaknesses of the remaining controls have been summarized into the following opportunities for improvement.

1. System Event Auditing

The ESCS web application does not have adequate event auditing controls to support the investigation of security incidents. OPM has not assessed the auditing capability of the web application to determine what events should be audited and under what circumstances.

NIST SP 800-53, Revision 4, control AU-2 (a., c, and d.) requires that the organization determines what events the information system is capable of auditing. The organization must determine which of those events will be audited by the system and under what circumstances and provide a rationale for why the selected auditable events are adequate to support the investigation of security incidents. NIST SP 800-53, Revision 4, control AU-3 states that "The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event."

The inability to audit events within the ESCS web application limits the artifacts that can be observed to investigate security incidents.

Recommendation 8

We recommend that OPM complete an assessment of the ESCS web application's auditing capability to determine what events should be audited by the system and under what circumstances.

OPM's Response:

"We concur. The remediation tasks to remediate this finding are actively in progress. Employee Services has developed a custom internal auditing capability. The decision on which auditable events will be logged by the system and under what circumstances is currently in progress."

Recommendation 9

We recommend that OPM implement the appropriate system auditing capabilities as determined by the assessment.

OPM's Response:

"We concur. The tasks to remediate this finding are in progress. Employee Services is implementing an auditing capability which reuses previously established code with slight modifications. The tailored auditing capability has been completed and is pending testing. It is scheduled to be fully implemented by early Fiscal Year 2022. The current and tailored auditing capability is a short-term solution. For the long-term solution, OPM will evaluate cloud-based options and adopt the appropriate audit capabilities of that solution."

2. System Inventory

OPM has not provided a definitive answer on what operating systems are being used within the ESCS system boundary. The ESCS's system documents contain the following conflicting inventories:

- The ESCS Contingency Plan has one inventory that states all servers are running Windows Server 2012 R2 and another inventory that states all servers are running Windows Server 2016;
- The ESCS Business Impact Analysis states that servers are running Windows Server 2016 and Red Hat Enterprise Linux 7;
- The ESCS SSP states that all systems are running Windows Server 2012; and
- The SSP and Contingency Plan state that the ESCS uses Oracle databases. However, OPM stated that the ESCS uses Microsoft SQL databases.

The ESCS does not have a system-level configuration management plan to identify and manage configuration items throughout the system development lifecycle. Shortly after we brought this opportunity for improvement to OPM's attention, affected documents were updated to reflect the current system inventory. These documents are awaiting approval before they can be finalized.

NIST SP 800-53, Revision 4, control CM-8 (a.) Information System Component Inventory, states that the organization "Develops and documents an inventory of information system components that: … accurately reflects the current information system ..." and "includes all components within the authorization boundary of the information system … ." NIST SP 800-53, Revision 4, control CM-9 (b.) Configuration Management Plan, states that "The organization develops, documents, and implements a configuration management plan for the

information system that … Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items ... ." NIST SP 800-53, Revision 4, defines configuration items as hardware, software, firmware, and documentation to be configuration-managed.

Failure to develop a system-level configuration management plan limits OPM's ability to maintain an accurate inventory of system components and supporting documentation.

Recommendation 10

We recommend that OPM develop a system-level configuration management plan for the ESCS that establishes a process for identifying and managing configuration items and documentation.

OPM's Response:

"We concur. Employee Services follows OPM's Enterprise Configuration Management Plan (ECM). All changes in the ESCS environment are subject to the ECM process. This process includes a change proposal, security impact analysis, testing, and approval prior to deployment in the production environment. All changes to ESCS are logged and tracked in the ECM portal."

OIG Comment:

The intent of this recommendation is for the ESCS to create a strategy for updating its various system documentation in the event of a significant system change. A system-level configuration management plan which includes configuration items as well as supporting documents will help the ESCS identify documentation requiring updates in the event of a significant system change.

Recommendation 11

We recommend that OPM document an inventory of information system components that accurately reflects the current information system.

OPM's Response:

"We concur. The Contingency Plan and the System Security Plan have been updated to accurately reflect the current inventory of the ESCS information system components. Both documents are currently pending review and signature by the System Owner. We will provide the documents as soon as they are signed."

3. Software License Tracking

OPM provided evidence that Employee Services maintains software license quantity

contracts. However, evidence was not provided demonstrating that software license usage within the ESCS system boundary is tracked. The usage of quantity-controlled software licenses is not documented.

NIST SP 800-53, Revision 4, control CM-10 (b.) Software Usage Restrictions, states that the organization "Tracks the use of software and associated documentation protected by quantity licenses … ."

Failure to track and document the use of software licenses limits OPM's ability to control unauthorized copying and distribution of that software.

Recommendation 12

We recommend that OPM track and document the usage of all quantity-controlled software licenses used within the ESCS system boundary.

OPM's Response:

"We concur. OPM will identify the software license in use and provide this evidence to support closure of the recommendation. Employee Services maintains a copy of the software requisition contract as well as a spreadsheet of where those two copies are in use. This information is reviewed annually when the support contract is renewed, or additionally as needed in the case of a new hire."

4. Logical Access Termination

OPM has not provided sufficient evidence demonstrating that access to the ESCS web application is disabled in a timely manner when a user's employment is terminated. OPM does not have a process to ensure access to the ESCS web application is disabled within 24 hours of receiving a termination notification.

NIST SP 800-53, Revision 4, control PS-4 (a.) Personnel Termination, states that upon termination of individual employment, the organization "Disables information system access within [the organization-defined time period]." The ESCS SCM states that "All accounts are disabled within 24 hours of receiving the notification."

Failure to disable information system access in a timely manner following termination of employment increases the risk of unauthorized access to the ESCS data.

Recommendation 13

We recommend that OPM establish a process to ensure access to the ESCS web application is disabled within 24 hours of receiving a termination notification.

OPM's Response:

"We concur. The ESCS administrators disable user accounts within 24 hours of receiving notification of the user's termination. Evidence has been provided to show that external and internal ESCS accounts are disabled upon notification. OPM will have the ability to capture and demonstrate the date/time stamps when auditing capabilities have been implemented in the production environment. Once the auditing capability is implemented, OPM will provide evidence to show the date/time stamp of account termination."

5. Unit Integration Testing

The ESCS SCM states that unit integration testing is performed for changes or modifications to the ESCS source code including upgrades and patches. However, OPM did not provide evidence that unit integration testing is performed. OPM does not have a security assessment plan which defines the testing process and documentation requirements for the ESCS web application development.

NIST SP 800-53, Revision 4, control SA-11 (a., b. c.) Developer Security Testing and Evaluation, states that the organization requires the developer to "Create and implement a security assessment plan; perform [unit; integration; system; regression] testing/evaluation at [the organization-defined depth and coverage] …" and "Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation … ."

Failure to create a security assessment plan increases the risk that adequate testing will not be performed when changes to source code have been made.

Recommendation 14

We recommend that OPM create and implement a security assessment plan for performing required testing and documenting results when changes are made to the ESCS web application source code.

OPM's Response:

"We concur. Functionality tests are conducted on ESCS to verify that the system works as intended prior to deployment. A unit testing plan will be established and employed to include unit testing and documentation of the results during configuration changes to the ESCS web application source code."

Appendix

August 23, 2021

Memorandum for: Eric W. Keehan
Group Chief, Information Systems Audits Group
Office of the Inspector General

From: Guy V. Cavillo
Chief Information Officer

Kristopher Goas
Supervisory HR Specialist, Employee Services

Subject: Management Response to the Draft Report on Information Technology Security Controls of the Executive Schedule C System (Report No. 4A-ES-00-21-020)

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 Executive and Schedule C System, Report No. 4A-ES-00-21-020, dated July 28, 2021.

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

Recommendation 1: We recommend that OPM update ESCS's public PIA to reflect the system's current operational environment.

Management Response: Based on the notice of Findings and Recommendations, shared with us by the CIO and Employee Services, we updated the ESCS PIA to reflect the current environment. The Chief Privacy Officer approved and signed the revised PIA, effective July 22, 2021 (see attached document) and in accordance with OPM practice, the final PIA was sent to the Director's office for instruction to the Office of Communications to post to the OPM public site. The PIA is now available for public viewing. As this issue was remediated, we ask that the recommendation be removed from the final report.

Recommendation 2: We recommend that OPM routinely review and update the ESCS SCM to ensure that controls are accurately documented and effectively satisfy all control requirements.

Management Response: We concur. The system ISSO, program office and process owners meet bi-weekly to review and update the ESCS security control matrix. The purpose of the bi-weekly meeting is to ensure that all controls are accurately documented in the SCM to a level that fully satisfies control requirements. The bi-weekly meetings will continue until all applicable ESCS security controls have been reviewed and verified with artifacts. The

meeting agenda and post-meeting recap document the remediation efforts discussed during the meeting. OPM will provide supporting artifacts with the completed SCM.

Recommendation 3: We recommend that OPM create a POA&M for all controls listed as "Planned" in the SCM, weaknesses identified during the last security controls assessment, and weaknesses identified during FY 2020 continuous monitoring.

Management Response: We concur. OPM requests that this recommendation be removed from the final audit report. OPM has documented the POA&Ms for all controls identified as planned in the SCM and the weaknesses previously identified in FY2020 continuous monitoring. The POA&Ms identified during the last security assessment have been reviewed to determine if they are applicable. These POA&Ms will be tracked and maintained as milestones are completed and updates are provided. Evidence of these POA&Ms are included with this report response.

Recommendation 4: We recommend that OPM perform and document a reassessment of the scheduled completion date for all open ESCS POA&Ms that have surpassed the scheduled completion date.

Management Response: We concur. The scheduled completion date that is initially provided during the evaluation and documentation of the POA&M signifies the date that Employee Services aims to resolve the vulnerability. Due to unexpected circumstances, such as unsuccessful remediations, limited resources, or additional time required to complete the tasks identified in the milestones, the scheduled completion date is often reevaluated. The revised date is tracked as the Expected Completion Date. OPM will review the original and revised dates to ensure that they are on or after the submission date.

Recommendation 5: We recommend that OPM establish and document configuration settings for technology products employed within the ESCS system boundary that reflect the most restrictive mode consistent with operational requirements.

Management Response: We concur. OPM will review the technology products contained within the ESCS system boundary, ensuring that this boundary is clearly defined and that all relevant inherited controls are considered. Once the technology products have been verified, we will establish and document the system specific configuration settings. Our target completion date for this recommendation is Fiscal Year 2022 Q3.

Recommendation 6: We recommend that OPM use privileged credentials to authenticate vulnerability scans of ESCS servers.

Management Response: We concur. OPM requests that this recommendation is removed from the final audit report. This finding was remediated on June 24, 2021. OPM has configured vulnerability scanning tools to execute privileged scans on ESCS as was previously configured. Documentation to show the updated scanning credentials is enclosed.

Recommendation 7: We recommend that OPM remediate the specific technical weakness discovered during this audit.

Management Response: We concur. A POA&M for the weakness has been documented and is being tracked. This POA&M has been discussed in the ESCS bi-weekly POA&M review meeting. An action plan is being set forth for remediation and is expected to be completed in FY22 Q1.

Recommendation 8: We recommend that OPM complete an assessment of the ESCS web application's auditing capability to determine what events should be audited by the system and under what circumstances.

Management Response: We concur. The remediation tasks to remediate this finding are actively in progress. Employee Services has developed a custom internal auditing capability. The decision on which auditable events will be logged by the system and under what circumstances is currently in progress.

Recommendation 9: We recommend that OPM implement the appropriate system auditing capabilities as determined by the assessment.

Management Response: We concur. The tasks to remediate this finding are in progress. Employee Services is implementing an auditing capability which reuses previously established code with slight modifications. The tailored auditing capability has been completed and is pending testing. It is scheduled to be fully implemented by early Fiscal Year 2022. The current and tailored auditing capability is a short-term solution. For the long-term solution, OPM will evaluate cloud-based options and adopt the appropriate audit capabilities of that solution.

Recommendation 10: We recommend that OPM develop a system-level configuration management plan for ESCS that establishes a process for identifying and managing configuration items and documentation.

Management Response: We concur. Employee Services follows OPM's Enterprise Configuration Management Plan (ECM). All changes in the ESCS environment are subject to the ECM process. This process includes a change proposal, security impact analysis, testing, and approval prior to deployment in the production environment. All changes to ESCS are logged and tracked in the ECM portal.

Recommendation 11: We recommend that OPM document an inventory of information system components that accurately reflects the current information system.

Management Response: We concur. The Contingency Plan and the System Security Plan have been updated to accurately reflect the current inventory of the ESCS information system components. Both documents are currently pending review and signature by the System

Owner. We will provide the documents as soon as they are signed.

Recommendation 12: We recommend that OPM track and document the usage of all quantity-controlled software licenses used within the ESCS system boundary.

Management Response: We concur. OPM will identify the software license in use and provide this evidence to support closure of the recommendation. Employee Services maintains a copy of the software requisition contract as well as a spreadsheet of where those two copies are in use. This information is reviewed annually when the support contract is renewed, or additionally as needed in the case of a new hire.

Recommendation 13: We recommend that OPM establish a process to ensure access to the ESCS web application is disabled within 24 hours of receiving a termination notification.

Management Response: We concur. The ESCS administrators disable user accounts within 24 hours of receiving notification of the user's termination. Evidence has been provided to show that external and internal ESCS accounts are disabled upon notification. OPM will have the ability to capture and demonstrate the date/time stamps when auditing capabilities have been implemented in the production environment. Once the auditing capability is implemented, OPM will provide evidence to show the date/time stamp of account termination.

Recommendation 14: We recommend that OPM create and implement a security assessment plan for performing required testing and documenting results when changes are made to the ESCS web application source code.

Management Response: We concur. Functionality tests are conducted on ESCS to verify that the system works as intended prior to deployment. A unit testing plan will be established and employed to include unit testing and documentation of the results during configuration changes to the ESCS web application source code.

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact Kristopher Goas at (724) 504-1182, Kristopher.Goas@opm.gov.

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: http://www.opm.gov/our-inspector-general/hotline-to-report-fraud-waste-or-abuse

By Phone: Toll Free Number: (877) 499-7295
Washington Metro Area (202) 606-2423

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