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

Final Audit Report

Subject:

AUDIT OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S COMMON SECURITY CONTROLS COLLECTION FY 2013

Report No. 4A-CI-00-13-036

Date: 10/10/13

--CAUTION--

This audit report has been distributed to Federal officials who are responsible for the administration of the audited program. This audit report may contain proprietary data which is protected by Federal law (18 U.S.C. 1905). Therefore, while this audit report is available under the Freedom of Information Act and made available to the public on the OIG webpage, caution needs to be exercised before releasing the report to the general public as it may contain proprietary information that was redacted from the publicly distributed copy.

Audit Report

U.S. OFFICE OF PERSONNEL MANAGEMENT

--

AUDIT OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S COMMON SECURITY CONTROL COLLECTION
FY 2013

WASHINGTON, D.C.

Report No. 4A-IS-00-13-036

Date: 10/10/13

Michael R. Esser
Assistant Inspector General
for Audits

--CAUTION--

This audit report has been distributed to Federal officials who are responsible for the administration of the audited program. This audit report may contain proprietary data which is protected by Federal law (18 U.S.C. 1905). Therefore, while this audit report is available under the Freedom of Information Act and made available to the public on the OIG webpage, caution needs to be exercised before releasing the report to the general public as it may contain proprietary information that was redacted from the publicly distributed copy.

Executive Summary

U.S. OFFICE OF PERSONNEL MANAGEMENT

--

AUDIT OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S COMMON SECURITY CONTROL COLLECTION

FY 2013

WASHINGTON, D.C.

Report No. 4A-IS-00-13-036

Date: 10/10/13

This final audit report discusses the results of our audit of the U.S. Office of Personnel Management's (OPM) Common Security Controls Collection (CSCC). Our conclusions are detailed in the "Results" section of this report.

CSCC Policies and Procedures

We believe that OPM's CSCC offers a conceptually comprehensive approach to effectively utilizing and testing a set of common information security controls.

CSCC Implementation

The CSCC adequately reflects the common controls that are provided by agency-wide policies and by physical facilities management. However, we do not believe that the CSCC accurately reflects the common controls provided by the agency's General Support Systems (GSS).

Use of the CSCC

The owners of OPM's major applications residing on the GSSs labeled at least several security controls as common that were not identified as common on the CSCC. As a result, these controls were inappropriately omitted from testing by the application owner.

Contents

Page

Introduction and Background

The Office of Personnel Management (OPM) operates approximately 50 major applications that support the agency's mission. This includes three general support systems (GSS) that host several smaller systems that leverage the centralized hardware, software, and personnel resources offered by the GSS. The GSSs are owned and operated by the Office of the Chief Information Officer (OCIO).

The Federal Information Security Management Act requires that all major applications be subject to routine security control testing. However, when a security control is provided by a GSS to all of the applications that it hosts (referred to as a "common" control), the individual application owners are not required to independently test this control, as that would be redundant of the OCIO's testing efforts.

In an effort to streamline the management of common controls, the OCIO created the Common Security Controls Collection (CSCC). The CSCC is intended to be a shared resource for all OPM security professionals and management to reduce duplicate efforts in the information system security control testing process. In addition to the common controls provided by the GSSs, the CSCC identifies the security controls that are addressed by agency-wide policies and procedures and by facilities management and various OPM buildings.

The CSCC was formally distributed in September 2012, and has since been used by application owners to facilitate their systems' security control tests.

Objectives

The objectives of this audit were to assess the quality of the CSCC and to evaluate the effectiveness of its use by information system owners. These objectives were met by:

- Meeting with OCIO personnel;
- Reviewing policies and guidance regarding the use of the CSCC; and
- Testing the CSCC elements for compliance with known regulations.

Scope and Methodology

This performance audit was conducted by the Office of the Inspector General (OIG) in accordance with 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 that we considered necessary. The audit documented the controls in place for the CSCC as of July 2013.

We considered the nature of the CSCC and the internal control structure of the OCIO in planning our audit procedures. These procedures were mainly substantive in nature, although we did gain an understanding of the management procedures and controls to the extent necessary to achieve our audit objectives.

Our audit evaluated the elements to create, attest, maintain, and utilize the CSCC. We looked at the CSCC at the time of publication as well as the implementation and use of the CSCC over a period of nine months since publication. We focused our review on the controls listed as common to the agency and those of the general support systems and did not conduct a review of the inherited controls or those controls attributable to physical locations.

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 came to our attention during our audit testing utilizing the computer-generated data to cause us to doubt its reliability. We believe that the data was sufficient to achieve the audit objectives. Except as noted above, the audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States.

Details of our audit findings and recommendations are located in the "Results" section of this report. Since our audit would not necessarily disclose all significant matters related to the CSCC, we do not express an opinion on the utilization of the CSCC as a whole, only the elements reviewed as a part of this audit.

The audit was conducted from February through October of 2013 in OPM's Washington, D.C. headquarters building.

Compliance with Laws and Regulations

In conducting the audit, we performed tests to determine whether OPM's management of the CSCC is consistent with applicable standards. Nothing came to our attention during this review to indicate that OPM is in violation of relevant laws and regulations.

Results

The sections below provide a summary of our audit findings and recommendations related to the creation and implementation of the CSCC.

I. CSCC Policies and Procedures

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," outlines a wide variety of information system security controls that should be implemented on all major applications.

OPM has three major general support systems (GSS) that each hosts a variety of independent applications supporting OPM's mission. Due to the shared hardware, software, and personnel resources maintained for each GSS, the applications residing on a GSS inherit some of the information security controls implemented from its parent system. Many OPM applications also obtain security controls provided by agency-wide policies and procedures and by the physical controls implemented at various OPM buildings.

In September 2012, OPM's OCIO published a catalog of agency-wide common security controls along with a guidance document labeled "Use of Common Security Controls Collection (CSCC)." The intent of the CSCC is to formally document the security controls that each GSS provides to the applications that reside on that GSS. As a result, the individual application owners will not have to routinely test those common security controls that are provided by the GSS, as this work is performed by the GSS owners.

We reviewed the OCIO's common controls documentation to verify that it provided OPM's security professionals and management adequate guidance to appropriately leverage the common controls provided by a GSS.

The guide provides the following:

- The background and purpose of the CSCC;
- The four step CSCC process;
- The intended use of the CSCC;
- The validation process for common controls;
- An explanation of the difference between common and inherited controls; and
- Instructions for implementing the CSCC.

We believe that OPM's CSCC offers a conceptually comprehensive approach to effectively utilizing and testing a set of common information security controls. However, the sections below detail several issues we detected in the actual implementation and use of the CSCC.

II. CSCC Implementation

While we believe that the CSCC adequately reflects the common controls that are provided by agency-wide policies and by physical facilities management, we do not believe that the CSCC accurately reflects the common controls provided by the agency's GSSs. OPM's OCIO contracted with the Bureau of Public Debt (BPD) to determine which information security controls are "common," and to also independently test these controls. Although it appears that the BPD performed some test work on all of the CSCC controls, we do not believe that the BPD adequately verified that each of these controls are, in fact, provided to every application that resides on each GSS.

As part of this audit we independently tested a sample of common controls, and found that each tested control was adequately implemented for the specific GSS hosting that control. However, our interviews with the GSS owners revealed that many of the controls listed as "common" on the CSCC are not enforced and/or available for each of the applications residing on the GSS. In other words, the CSCC labels certain controls as common that really should have been implemented for each individual application (referred to as system-specific controls).

NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems, defines a common security control as having "the following properties: [i] The development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owners . . .); and [ii] The results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control has been applied."

Incorrectly labeling security controls as common increases the likelihood that these controls are not properly implemented and tested at the application level, which in turn increases the risk of sensitive data breaches.

Recommendation 1

We recommend that the OCIO meet with each GSS owner to determine which information security controls are provided to every application hosted by that GSS. The GSS owners should formally acknowledge this updated list of controls, and the results should be published in a new CSCC.

OCIO Response:

"The security staff will meet with General Support System providers to document and discuss the recommended changes. The Common Controls Procedures and Catalog will be updated and republished reflecting all changes.

The CIO agrees that in some circumstances, depending on the implementation of the system and/or categorization the GSS cannot provide all the security objectives of a listed Security Control in the CSCC. For the instance where the GSS (LAN/WAN) has a lower categorization than the Major Application using the Security Control . . . the Assessor

(BPD) was instructed to assess each of the control[s] at the HIGH Categorization implementation, thus alleviating any issue with Major Applications with a higher Categorization than that of the GSS. Some Major Applications may choose to implement Security Controls and Mechanisms that superimpose, complement or enhance those provided by the GSS, but these implementations are at the purview of the Major Application's System Owner. The CIO agrees that there needs to be some collaboration on the part of the System Owners and the Control Provider (GSS) to assure that the controls that the System Owner is indicating as 'inherited' or 'hybrid' are applicable to their implementations and available from the Control Provider."

OIG Reply:

As part of the audit resolution process for this recommendation and all subsequent recommendations to which OCIO agrees, please provide OPM's Internal Oversight and Compliance (IOC) division with evidence supporting the corrective action taken.

Recommendation 2

We recommend that no OPM application rely on the general support system portion (LAN-WAN, ESI, Macon) of the current version of the CSCC when performing any form of security control testing. This recommendation is effective immediately, and should not be closed until Recommendation 1 is completely implemented.

OCIO Response:

"The CIO agrees that there needs to be better information relating to the assumption of 'inherited' and/or 'hybrid' controls from any of the Control Providers (LAN/WAN, ESI and MACON GSS). The security team will work with the GSS providers to update the necessary controls."

III. Use of the CSCC

As stated above, the intent of the CSCC is to reduce duplicate efforts in the testing of information security controls. If a security control is provided by a GSS, then the applications residing on that GSS do not need to test that control.

Section II describes our concern that the CSCC does not accurately reflect the security controls that are truly common to all systems residing on each GSS. That issue aside, we also determined that individual application owners are not appropriately using the current version of the CSCC.

The Information System Security Plan (ISSP) of each major OPM application describes the security controls that are in place for that system. We examined the ISSP for each OPM application that resides on a GSS, and mapped the security controls detailed in the ISSP to the CSCC. Our review indicated that the owners of every one of these applications had labeled at least several security controls as common that were not identified as common on the CSCC. As a result, these controls were inappropriately omitted from testing by the application owner.

> We acknowledge that there are instances when an application can inherit a control from a GSS, even if that control is not a universal common control to all other applications on that GSS. However, in these instances the CSCC cannot be leveraged, and the application owners must work with the GSS owners to determine exactly which controls are provided by the GSS. We believe that formalizing this process will reduce the risk that controls will be mislabeled as common or inherited, and that every control will be tested either at the GSS or application level.

Recommendation 3

Once the new CSCC is published, we recommend that the owners of all applications residing on a GSS update the system's ISSP to identify and immediately test all controls that were previously mislabeled as a common control.

OCIO Response:

"The CIO agrees that additional documentation and training on the use of the Common Security Controls in the CSCC should be given and that additional scrutiny of System Security Plans to include a review of Agency Common Controls is warranted.

The CIO will [be] republishing the CSCC to identify each Security Control, if any, that were incorrectly identified as Common and appropriately notify each system owner with their responsibility to assess each control and update their SSP respectively.

Controls that were mislabeled will be included in the assessment of controls under the Information Security Continuous Monitoring (ISCM) Program."

Recommendation 4

We recommend that OCIO update the CSCC procedures to require application owners to seek formal acknowledgement from GSS owners when inheriting security controls from that GSS that are not common to all other applications. This process should require the use of a template that is signed by the GSS owner as their acknowledgement that the controls are provided to that application.

OCIO Response:

"The CSCC Process currently has a process to have the Major Application verify that controls that are marked as 'Inherited' in the CSCC must be verified with the GSS System Owner for their use. The security team will develop a template for GSS owners to acknowledge inheritable controls."

Major Contributors to this Report

This audit report was prepared by the U.S. Office of Personnel Management, Office of the Inspector General, Information Systems Audits Group. The following individuals participated in the audit and the preparation of this report:

- Lewis F. Parker, Deputy Assistant Inspector General for Audits
- [redacted] Senior Team Leader
- [redacted], Lead IT Auditor In Charge
- [redacted], IT Auditor

Appendix

9/25/13

MEMORANDUM FOR LEWIS F. PARKER, JR
DEPUTY ASSISTANT INSPECTOR GENERAL
FOR AUDITS

FROM: CHARLES R. SIMPSON
ACTING, CHIEF INFORMATION OFFICER

Subject: CIO Responses to OIG Audit 4A-CI-00-13-036

Recommendation 1

We recommend that the OCIO meet with each GSS owner to determine which information security controls are provided to every application hosted by that GSS. The GSS owners should formally acknowledge this updated list of controls, and the results should be published in a new CSCC.

CIO Response:

> The security staff will meet with General Support System providers to document and discuss the recommended changes. The Common Controls Procedures and Catalog will be updated and republished reflecting all changes.
>
> The CIO agrees that in some circumstances, depending on the implementation of the system and/or categorization the GSS cannot provide all the security objectives of a listed Security Control in the CSCC. For the instance where the GSS (LAN/WAN) has a lower categorization than the Major Application using the Security Control. In this circumstance the Assessor (BPD) was instructed to assess each of the control at the HIGH Categorization implementation, thus alleviating any issue with Major Applications with a higher Categorization than that of the GSS. Some Major Applications may choose to implement Security Controls and Mechanisms that superimpose, complement or enhance those provided by the GSS, but these implementations are at the purview of the Major Application's System Owner. The CIO agrees that there needs to be some collaboration on the part of the System Owner and the Control Provider (GSS) to assure that the controls that the System Owner is indicating as "inherited" or "hybrid" are applicable to their implementations and available from the Control Provider.

Recommendation 2

We recommend that no OPM application rely on the general support system portion (LAN-WAN, ESI, Macon) of the current version of the CSCC when performing any form of security control testing. This recommendation is effective immediately, and should not be closed until Recommendation 1 is completely implemented.

CIO Response:

> The CIO agrees that there needs to be better information relating to the assumption of "inherited" and/or "hybrid" controls from any of the Control Providers (LAN/WAN, ESI and MACON GSS). The security team will work with the GSS providers to update the necessary controls.

Recommendation 3

Once the new CSCC is published, we recommend that the owners of all applications residing on a GSS update the system's ISSP to identify and immediately test all controls that were previously mislabeled as a common control.

CIO Response:

> The CIO agrees that additional documentation and training on the use of the Common Security Controls in the CSCC should be given and that additional scrutiny of System Security Plans to include a review of Agency Common Controls is warranted.
>
> The CIO will republishing the CSCC to identify each Security Control, if any, that were incorrectly identified as Common and appropriately notify each system owner with their responsibility to assess each control and update their SSP respectively.
>
> Controls that were mislabeled will be included in the assessment of controls under the Information Security Continuous Monitoring (ISCM) Program.

Recommendation 4

We recommend that OCIO updated the CSCC procedures to require application owners to seek formal acknowledgement from GSS owners when inheriting security controls from that GSS that are not common to all other applications. This process should require the use of a template that is signed by the GSS owner as their acknowledgement that the controls are provided to that application.

CIO Response:

> The CSCC Process currently has a process to have the Major Application verify that controls that are marked as "Inherited" in the CSCC must be verified with the GSS System Owner for their use. The security team will develop a template for GSS owners to acknowledge inheritable controls.