



Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

Audit Summary

Security of Common
Control Providers

142319 August 2024



Office of the Inspector General

SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: August 28, 2024

Refer to: 142319

To: Martin O'Malley
Commissioner

From: Michelle L. Anderson *Michelle L. Anderson*
Assistant Inspector General for Audit
as Acting Inspector General

Subject: Security of Common Control Providers

The attached final report summarizes Ernst & Young LLP's (Ernst & Young) review of the information technology security controls of common control providers. Under a contract the Office of Audit monitored, Ernst & Young, an independent certified public accounting firm, reviewed the security of common control providers. Ernst & Young interviewed Social Security Administration staff and management and reviewed evidence the Agency provided.

Ernst & Young's audit results contain information that, if not protected, could be used to adversely affect SSA's information systems. In accordance with government auditing standards, we have transmitted Ernst & Young's detailed findings and recommendations to Agency management and excluded from this summary sensitive information because of the potential damage if the information is misused. The omitted information neither distorts the audit results described in this report nor conceals improper or illegal practices.

If you wish to discuss the final report, please call me or have your staff contact Jeffrey Brown, Deputy Assistant Inspector General for Audit.

Attachment

TABLE OF CONTENTS

Objective.....	1
Background.....	1
Ernst & Young's Scope and Methodology	2
Our Evaluation of Ernst & Young's Performance.....	2
Results of Ernst & Young's Review	3
Ernst & Young's Recommendations.....	3
Agency Comments.....	3
Office of the Inspector General's Comments.....	3
Appendix A – Ernst & Young's Scope and Methodology	A-1
Appendix B – Agency Comments.....	B-1

ABBREVIATIONS

CCP	Common Control Provider
GAO	Government Accountability Office
OIG	Office of the Inspector General
NIST	National Institute for Standards and Technology
SSA	Social Security Administration

OBJECTIVE

The objective was to determine whether the information technology security controls of common control providers (CCP) are designed, implemented, and operating effectively.

BACKGROUND

Common controls are security or privacy controls that can be inherited by one or more information systems. Common controls may include National Institute for Standards and Technology (NIST) security controls.¹ For example, if a system is kept in a Social Security Administration (SSA) data center, an Agency component manages that data center's physical access and environmental protection controls (fire suppression or heating, ventilation, and air conditioning).

Organizations identify and select the set of common controls and allocate those controls to the organizational entities designated as CCPs. CCPs are responsible for:

- documenting common controls in security plans;
- ensuring the common controls are implemented and assessed for effectiveness by qualified assessors and findings are documented in assessment reports;
- producing a plan of action and milestones for common controls determined to have unacceptable deficiencies and targeted for remediation;
- requesting authorization for the common controls from the designated authorizing official; and
- monitoring control effectiveness on an ongoing basis.

SSA instructs CCP Security Authorization Managers to make plans, assessment reports, and plans of action and milestones for common controls (or a summary of such information) available to system owners. Authorizing officials can use these to guide and inform authorization decisions for systems that inherit common controls.

Security Authorization Managers assess CCPs to determine whether the controls available for inheritance satisfy the security and privacy requirements for organizational systems and the environments in which those systems operate. When Security Authorization Managers determine the common controls the organization provides are insufficient, they document a risk. All systems that inherit the insufficient common control inherit the risk. When information systems inherit those controls and risks, system owners can supplement the common controls with system-specific or hybrid controls to achieve the required protection for their systems or accept greater risk with the organization's acknowledgment and approval.

SSA documents its inheritance structure using a third-party tool for cyber-risk management and compliance automation. Systems owners can request control inheritance using a third-party tool, and the CCP Security Authorization Manager can approve or reject inheritance requests.

¹ NIST, *Security and Privacy Controls for Information Systems and Organizations*, SP 800-53, Rev. 5 (December 2020).

ERNST & YOUNG’S SCOPE AND METHODOLOGY

Under a contract we monitored, Ernst & Young LLP (Ernst & Young) conducted this performance audit in accordance with generally accepted government auditing standards.² Ernst & Young evaluated SSA’s common controls in accordance with specified areas outlined in the Statement of Work’s Planned Scope and Methodology.³ These specified areas were mapped to the Framework. Ernst & Young also completed the following:

- conducted system walkthroughs with SSA personnel to understand common controls and identified relevant policies, procedures, and processes;
- observed controls as they occurred and inspected evidence to support the controls’ implementation; and
- performed detailed technical security controls testing with SSA’s information system staff knowledge and consent.

See Appendix A for details of Ernst & Young’s scope and methodology.

OUR EVALUATION OF ERNST & YOUNG’S PERFORMANCE

To monitor Ernst & Young’s review, we:

- reviewed Ernst & Young’s approach and planning;
- evaluated Ernst & Young personnel’s qualifications and independence;
- monitored Ernst & Young’s progress;
- examined Ernst & Young’s documentation and deliverables to ensure they complied with our requirements;
- coordinated the issuance of Ernst & Young’s results; and
- performed other procedures as deemed necessary.

We did not conduct our review of Ernst & Young’s work under generally accepted government auditing standards. Our review was not intended to enable us to express, and accordingly we do not express, our own opinion about whether the information technology security controls of CCPs are designed, implemented, and operating effectively. However, our monitoring review, as qualified above, disclosed no instances where Ernst & Young did not comply with our requirements.

² Government Accountability Office, *Government Auditing Standards, 2018 Revision, GAO-21-368G* (Technical Update April 2021).

³ Contract Number: GS-00F-290CA, Task Order Number 28321323FDX030009.

Ernst & Young's audit results contain information that, if not protected, could result in adverse effects to the Agency's information systems. In accordance with government auditing standards,⁴ we have separately transmitted to SSA management Ernst & Young's detailed findings and recommendations. We excluded from this summary certain sensitive information because of the potential damage that could result if the information is misused. We have determined the omitted information neither distorts the audit results described in this report nor conceals improper or illegal practices.

RESULTS OF ERNST & YOUNG'S REVIEW

Ernst & Young concluded SSA's information technology security controls of CCPs were not designed and operating as intended. Ernst & Young concluded SSA did not effectively design its CCP program environment. In addition, in some instances, SSA had not implemented policies, procedures, and practices to fully address requirements outlined in SSA's Information Security Policy and related NIST guidance. Specifically, Ernst & Young noted SSA had not:

- Defined processes for communicating inherited risks from Federal Risk and Authorization Management Program CCPs so they could be considered in the design and implementation of information technology cyber-security control by system owners.
- In some instances, (1) updated the system security plan documentation to identify control implementation requirements for all required controls or (2) maintained evidence to support the performance of continuous monitoring evaluations for CCPs.

ERNST & YOUNG'S RECOMMENDATIONS

Ernst & Young provided four recommendations to SSA to address the identified findings related to CCPs' security controls. Ernst & Young transmitted the recommendations to SSA management separately.

AGENCY COMMENTS

SSA agreed with Ernst & Young's recommendations and responded under separate cover. See Appendix B for the full text of SSA's comments on this summary.

OFFICE OF THE INSPECTOR GENERAL'S COMMENTS

SSA houses sensitive information about each person who has been issued a Social Security number. Without appropriate security, the Agency's systems, and the sensitive data they contain, are at risk. As such, it is imperative that SSA take actions related to CCP security controls to ensure the confidentiality, integrity, and availability of the Agency systems and data.

⁴ GAO, *Government Auditing Standards, 2018 Revision*, GAO-21-368G, 9.66, pp. 209 and 210 (Technical Update April 2021).

Appendix A – ERNST & YOUNG’S SCOPE AND METHODOLOGY

Objectives and Scope

The purpose of Ernst & Young’s common control provider (CCP) Supplemental In-Depth Performance Audit is to determine whether the Social Security Administration (SSA) information technology security controls of CCPs are designed, implemented, and operating effectively, to ensure the confidentiality, integrity, and availability of the agency’s information system are adequate.

Methodology

To accomplish the objectives, Ernst & Young performed the procedures outlined in the Statement of Work’s¹ Planned Scope and Methodology. Below is a list of criteria Ernst & Young used to conduct the CCP performance audit:

- Federal Risk and Authorization Management Program *Security Assessment Framework; System Security Plan Baseline Template; and Continuous Monitoring Strategy & Guide.*
- Government Accountability Office (GAO), *Government Auditing Standards*, Chapters 8 and 9.
- National Institute of Standards and Technology (NIST), *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 5.
- NIST *Framework for Improving Critical Infrastructure Cybersecurity* version 1.1.
- SSA policies and procedures.

This included considering the three cloud service models used in the SSA environment: (1) Infrastructure as a Service, (2) Platform as a Service, and (3) Software as a Service. Ernst & Young conducted walkthroughs with SSA personnel to understand the Agency’s cloud CCP and identified relevant policies, procedures, and processes. In addition, Ernst & Young observed controls as they occurred and inspected evidence to support the control’s implementation.

Ernst & Young evaluated the CCP’s program implementation of the Agency’s information security program in accordance with specified areas mapped to the NIST Framework, Version 1.1 dated April 16, 2018.²

- Identify:
 - Governance: Determine whether SSA had implemented a Risk Management Strategy for CCP use, including whether system owners’ roles and responsibilities had been adequately defined.
 - Risk Assessment: Determine whether SSA had implemented a process for the documentation, review, and communication of risk identified in CCPs.

¹ Contract Number: GS-00F-290CA, Task Order Number 28321323FDX030009.

² NIST, *Cybersecurity Framework V1.1* /www.nist.gov/cyberframework/csf-11-archive (April 2018).

- Risk Management Strategy: Determine whether the system had implemented logical access controls, role-based access, segregation of duties, and privileged account management controls.

Ernst & Young considered suggested controls outlined in the NIST cyber-security and privacy framework profile,³ along with the security and privacy control baselines identified in NIST 800-53 for the Government and tailored this guidance by risk to assist SSA in the control selection process. Additionally, Ernst & Young considered the Framework to NIST SP 800-53, Revision 5, mapping to identify additional controls to test to meet its audit objective.

Ernst & Young conducted this performance audit in accordance with *Government Auditing Standards*. Those standards require that Ernst & Young plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for its findings and conclusions based on the audit objective. Ernst & Young believes the evidence obtained provides a reasonable basis for its findings and conclusions based on the audit objective.

³ NIST, *Security and Privacy Controls for Information Systems and Organizations*, SP 800-53, Rev. 5 (December 2020).

Appendix B – AGENCY COMMENTS



SOCIAL SECURITY

MEMORANDUM

Date: July 30, 2024

Refer To: TQA-1

To: Michelle L. H. Anderson
Acting Inspector General

From: Dustin Brown 
Acting Chief of Staff

Subject: Office of the Inspector General Summary Report, “Security of Common Control Providers”
(142319) – INFORMATION

Thank you for the opportunity to review the summary report. We have no comments.

Please let me know if I can be of further assistance. Your staff may direct inquiries to Hank Amato, Director of the Audit Liaison Staff, at (407) 765-9774.



Mission:

The Social Security Office of the Inspector General (OIG) serves the public through independent oversight of SSA's programs and operations.

Report:

Social Security-related scams and Social Security fraud, waste, abuse, and mismanagement, at oig.ssa.gov/report.

Connect:

[OIG.SSA.GOV](https://oig.ssa.gov)


Visit our website to read about our audits, investigations, fraud alerts, news releases, whistleblower protection information, and more.

Follow us on social media via these external links:

 @TheSSAOIG

 OIGSSA

 TheSSAOIG

 Subscribe to email updates on our website.